

### **REMARKS**

Claims 1-53 are pending and were rejected. Claims 1, 2, 3, 5, 6, 18, 22, 31, 36, 44, 46, and 51 were amended. Claim 53 was amended in Applicants' Response to Office Action filed March 22, 2006, but it is not known if the amendment to claim 53 has been entered by the Examiner. No claims were cancelled. Thus claims 1-53 remain pending.

#### **Requirement for Information under 37 CFR § 1.105**

The Examiner has required the Applicants to provide a copy of the non-patent literature "Entity Authentication Using Public Key Cryptography" 1997 February 18<sup>th</sup> US Department of Commerce, (Attached as Exhibit "A") and "Three Pass Authentication" of ISO/IEC 9798-3, "Information technology-Security techniques-Entity Authentication-Part 3: Mechanisms using digital signature techniques," 1993 and 1998 (Attached as Exhibit "B").

Applicants do not clearly understand why the Examiner has required the Applicants to provide a copy of "Entity Authentication Using Public Key Cryptography," as the Examiner has included a copy of this reference when transmitting the Office Action to the Applicants. However, Applicants include a copy of this reference with the other required reference ISO/IEC 9798-3, "Information technology-Security techniques-Entity Authentication-Part 3: Mechanisms using digital signature techniques" 1998 attached to this Response. The 1993 version of ISO/IEC 9798-3 required to be submitted is not readily available to the parties from which it was requested.

The Examiner has also required that, where the claimed invention is an improvement over stated non-patent literature, Applicants identify what is being improved. Applicants note that the claimed invention is not an improvement over the stated patent literature in that aspects of the invention are orthogonal to the stated non-patent literature.

#### **Oath/Declaration**

The Examiner contends that the oath or declaration is defective. Applicants contend, however, that the present application has been filed correctly according to the Manual of Patent

Examining Procedure § 409.03. If a joint inventor refuses to join in an application for patent, the application may be made by the other inventors on behalf of themselves and the omitted inventor. MPEP § 409.03. Applicants filed a Response to Notice to File Missing Parts of Application on January 31, 2002 containing, among other documents, a declaration in compliance with 37 CFR § 1.63, a Petition for Acceptance of National Application without Participation of One or More Inventor Under 37 CFR § 1.47, and a Declaration of Louis Brucculeri in Support of Petition under 37 CFR § 1.47). The Examiner will note that the declaration includes each requirement cited by the Examiner in paragraph 3 of the Office Action, except as to where a requirement is superseded by the procedures of 37 CFR § 1.47. Application papers submitted by Applicants were forwarded to the Office of Petitions for a determination of whether the papers were proper, complete, and acceptable pursuant to 37 CFR § 1.47 and for a decision on the petition before the application was sent to the Technology Center. The Office of Petitions granted Applicants' petition by issuing a "Decision According Status Under 37 CFR § 1.47(a)" ("Decision") on August 23, 2002. The Decision explicitly states that the declaration of Louis Brucculeri filed June 6, 2002 has been found in compliance with 37 CFR § 1.63. For the Examiner's convenience, copies of the petition and the declaration are attached to this reply (Attached as Exhibit "C").

Rejections under 35 U.S.C. § 112, First Paragraph

Claims 51, 52, and 53

Claim 51 stands rejected under 35 USC § 112, first paragraph, as failing to comply with the enablement requirement. Claim 51 has been amended to correct the typographical error causing the enablement rejection and should now be allowed. Claims 52 and 53 stand rejected under 35 USC § 112, first paragraph, due to their dependence on independent claim 51. As claim 51 is now allowable, claims 52 and 53 should also be allowed. Applicants therefore request the withdrawal of the rejections under 35 USC § 112, first paragraph, and the allowance of claims 51, 52, and 53.

Rejections under 35 U.S.C. § 112, Second Paragraph

The Examiner has rejected various claims in the present application under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Applicants note that the examiner should allow claims which define the patentable subject matter with a reasonable degree of particularity and distinctness. MPEP § 2173.02. “Some latitude in the manner of expression and the aptness of terms should be permitted even though the claim language is not as precise as the examiner might desire.” *Id.* “Only when a claim remains insolubly ambiguous without a discernible meaning after all reasonable attempts at construction must a court declare it indefinite.” *Metabolite Labs., Inc. v. Lab. Corp. of Am. Holdings*, 370 F.3d 1354, 1366, 71 USPQ2d 1081, 1089 (Fed. Cir. 2004).

Accordingly, a claim term that is not used or defined in the specification is not indefinite if the meaning of the claim term is discernible. *Bancorp Services, L.L.C. v. Hartford Life Ins. Co.*, 359 F.3d 1367, 1372, 69 USPQ2d 1996, 1999-2000 (Fed. Cir. 2004) (holding that the disputed claim term “surrender value protected investment credits” which was not defined or used in the specification was discernible and hence not indefinite because “the components of the term have well recognized meanings, which allow the reader to infer the meaning of the entire phrase with reasonable confidence”).

MPEP § 2173.02. In light of the above, Applicants contend that none of the claims listed by the Examiner are indefinite as written. However, in an attempt to cooperate with the Examiner to improve the clarity or precision of the language used, Applicants have amended some of the claims which the Examiner regards as indefinite. In amending these claims, however, Applicants in no way intend to narrow the scope of any claim. The amendments made in regard to the Examiner's comments maintain the scope of the original claims while making the invention more clearly described for the Examiner.

Claims 1, 3, 4-6, 10-13, 21-23, 26, 31-37, 40, and 45-50

Claims 1, 3, 4-6, 10-13, 21-23, 26, 31-37, 40, and 45-50 stand rejected under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. The Office Action on page 5, paragraph 4, states that the terms “first type derivative,” “second type derivative,” and “third

type derivative” are indefinite, because “the instant specification only provides examples of ‘derivatives’ and provides neither a definition or the total number of possible derivatives.

Definiteness of claim language must be analyzed in light of the content of the particular application disclosure; the teachings of the prior art; and the claim interpretation that would be given by one possessing the ordinary level of skill in the pertinent art at the time the invention was made. MPEP § 2173.02. The instant specification, at paragraph [00145], discloses derivatives “created through differing derivation schemes (type 1 and type 2 respectively).” Various numbered types of derivatives are discussed throughout the specification. As disclosed in paragraph [00141] of the specification, these derivatives can be anything based on a specific piece of information, including an encryption, encoding, checksum, or hash, or even an encryption or encoding of a checksum or hash. The components of the terms “first type derivative,” “second type derivative,” etc., have well recognized meanings, which allow the reader to infer the meaning of the entire phrase with reasonable confidence. This is especially true when reading the terms in light of the instant specification. Those of skill in the art, therefore, will recognize that the convention employed by Applicants of referring to derivations as a “first type derivative,” “second type derivative,” etc., refer to derivatives resulting from derivation schemes that are not necessarily identical (e.g., a first type of derivation scheme, a second type of derivation scheme, etc.). As such, the scope of the claimed subject matter in the above claims can be determined by one having ordinary skill in the art. Applicants therefore request the withdrawal of the rejections under 35 USC § 112, second paragraph, and the allowance of claims 1, 3, 4-6, 10-13, 21-23, 26, 31-37, 40, and 45-50.

#### Claims 1 and 7

Claims 1 and 7 stand rejected under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. The Office Action on page 5, paragraph 4, states that the term “pre-defined information” is indefinite, because the claims do not state what time, event, or action the information is defined before. Applicants note that definiteness of claim language must be analyzed in light of the content of the particular application disclosure; the teachings of the prior art; and the claim interpretation that would be given by one possessing the ordinary level of skill

in the pertinent art at the time the invention was made. MPEP § 2173.02. “[P]re-defined information,” as used in Applicants’ specification and the above rejected claims, is a well-known concept in the prior art. “[P]re-defined information” means information not directly created by an authentication process. As such, the scope of the claimed subject matter in the above claims can be determined by one having ordinary skill in the art. Applicants therefore request the withdrawal of the rejections under 35 USC § 112, second paragraph, and the allowance of claims 1 and 7.

#### Claim 2

Claim 2 stands rejected under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. The Office Action on page 6, paragraph 4, states that claim 2 is unclear, as it states that the first port and the second port are the same port, and it is unclear to the Examiner how two distinct ports could be one port. Claim 1 has been amended for clarification that the two ports of claim 1 are not necessarily distinct, that is, that the two ports of claim 1 may or may not be distinct. Claim 2 therefore adds the limitation that they are not distinct, *i.e.*, they are the same port. Claim 2 is not indefinite, as the claims are amended, and therefore should be allowed. Applicants therefore request the withdrawal of the rejection under 35 USC § 112, second paragraph, and the allowance of claim 2.

#### Claim 3

Claim 3 stands rejected under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. The Office Action on page 6, paragraph 4, states that the term “nature” is indefinite. Claim 3 has been amended, as explained above, to make clear Applicants’ invention. Claim 3 is not indefinite as amended and therefore should be allowed. Applicants therefore request the withdrawal of the rejection under 35 USC § 112, second paragraph, and the allowance of claim 3.

Claims 5, 6, 18, 22, 31, 36, 44 and 46

Claims 5, 6, 18, 22, 31, 36, 44 and 46 stand rejected under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. The Office Action on page 6, paragraph 4, states that the term “associated” is indefinite. The above claims have been amended, as explained above, to make clear Applicants’ invention. The claims are not indefinite as amended and therefore should be allowed. Applicants therefore request the withdrawal of the rejections under 35 USC § 112, second paragraph, and the allowance of claims 5, 6, 18, 22, 31, 36, 44 and 46.

Claim 50

Claim 50 stands rejected under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. The Office Action on page 6, paragraph 4, states that the phrase “communication having a recognized purpose and an additional purpose” is indefinite, because every communication has a purpose. In the method of claim 50, however, a communication may have more than one purpose, and these purposes may be interpreted as a recognized purpose and an additional purpose, with the additional purpose being a request for authentication command. The scope of the claimed subject matter in the above claims can therefore be determined by one having ordinary skill in the art. Claim 50, therefore, is not indefinite and should be allowed. Applicants request the withdrawal of the rejection under 35 USC § 112, second paragraph, and the allowance of claim 3.

Claim 53

Claim 53 stands rejected under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. The Office Action on page 7, paragraph 4, states that the phrase “higher world wide name” is indefinite. Claim 53 has been amended, as explained above, to make clear Applicants’ invention. Claim 53 is not indefinite as amended and therefore should be allowed.

Applicants therefore request the withdrawal of the rejections under 35 USC § 112, second paragraph, and the allowance of claim 53.

Rejections under 35 U.S.C. § 103

The Examiner has the burden to establish a prima facie case of obviousness. MPEP § 2142. To establish a prima facie case of obviousness under 35 U.S.C. § 103, three criteria must be met. *Id.* The first element of a prima facie case of obviousness under 35 U.S.C. § 103 is that there must be a suggestion or motivation to combine the references. *In re Vaeck*, 947 F.2d 488, 493, 20 USPQ2d 1438, 1442 (Fed. Cir. 1991). The second element of a prima facie case of obviousness under 35 U.S.C. § 103 is that there must be a reasonable expectation of success in the proposed combination of the references. *In re Merck & Co., Inc.*, 800 F.2d 1091, 1097, 231 USPQ 375, 379 (Fed. Cir. 1986). The third element of a prima facie case of obviousness under 35 U.S.C. § 103 is that the proposed combination of the references must teach or suggest all of Applicants' claim limitations. *In re Royka*, 490 F.2d 981, 985, 180 USPQ 580, 583 (CCPA 1974).

Claims 1-19, 21-32, and 34-53

Claims 1-19, 21-32, and 34-53 stand rejected in the Office Action under § 103(a) as being unpatentable over U.S. Patent 5,473,599 to Li ("Li") in view of "Entity Authentication using Public Key Cryptography" by William Daley ("Daley"). Applicants respectfully traverse each rejection.

Claims 20 and 33

Claims 20 and 33 stand rejected in the Office Action under § 103(a) as being unpatentable over Li in view of Daley in view of JP02001148697A. Applicants respectfully traverse each rejection.

No Suggestion or Motivation to Combine

To establish a prima facie case of obviousness, there must be a suggestion or motivation to modify Li. *In re Vaeck*, 947 F.2d 488, 493, 20 USPQ2d 1438, 1442 (Fed. Cir. 1991). The suggestion or motivation to modify Li must come from the teaching of the cited art itself or

reasoned from knowledge generally available to one of ordinary skill in the art, established scientific principles, or legal precedent established by prior case law. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). The Examiner must explicitly point to the teaching suggesting the proposed modification, and the Examiner must present a convincing line of reasoning supporting the rejection. *Ex parte Clapp*, 227 USPQ 972 (Bd. Pat. App. & Inter. 1985). Absent such a showing, the Examiner has impermissibly used “hindsight” occasioned by Applicants’ own teaching to reject the claims. *In re Surko*, 11 F.3d 887, 42 USPQ2d 1476 (Fed. Cir. 1997); *In re Vaeck*, 947 F.2d 488m 20 USPQ2d 1438 (Fed. Cir. 1991); *In re Gorman*, 933 F.2d 982, 986, 18 USPQ2d 1885, 1888 (Fed. Cir. 1991); *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990); *In re Laskowski*, 871 F.2d 115, 117, 10 U.S.P.Q.2d 1397, 1398 (Fed. Cir. 1989).

There is no suggestion or motivation to modify Li. Li discloses a system and protocol for routing data packets from a host on a LAN through a virtual address belonging to a group of routers. The present invention claims security enhancements for a networking environment. Li is a system for increasing reliability of LAN communications through a router by switching to another working router if the primary router fails. The routers of Li periodically send “hello” messages to each other so that the operability of the router sending the messages will be known by the other routers. Li does not suggest or provide motivation for security, let alone the switch-level security of the present invention. Li, in fact, teaches away from security, as is reinforced by the disclosure in Li of sending hello messages to all routers using an IP multicast address and the use of the same weak authentication (password) for each router in the group. Furthermore, readers of skill in the art will recognize that the authentication disclosed in Li is for the purpose of preventing messages received from routers outside of the defined group from inadvertently being perceived as messages from routers within a defined group. Again, this authentication is for reliability purposes and not for security, as suggested by the weak authentication disclosed in Li. Thus, there is no suggestion or motivation to modify Li. The lack of a suggestion or motivation to modify Li is sufficient by itself to make the above claims allowable. As such, the rejection of claims 1-53 should be withdrawn and the claims should be allowed.



### No Reasonable Expectation of Success

To establish a prima facie case of obviousness, there must be a reasonable expectation of success in the proposed modification of Li. *In re Merck & Co., Inc.*, 800 F.2d 1091, 1097, 231 USPQ 375, 379 (Fed. Cir. 1986). There can be no reasonable expectation of success in a proposed modification if the proposed modification changes the principle of operation of Li. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

There can be no reasonable expectation of success in a proposed combination of a system and process for routing data packets from a host on a LAN through a virtual address belonging to a group of routers of Li with the strong authentication protocols of Daley to produce enhancement in switch-level security in a network environment as claimed in the present application. On the contrary, incorporating the 'strong authentication protocols' of Daley in the system and process for routing data packets from a host on a LAN through a virtual address belonging to a group of routers of Li would clearly change the principle of operation of Li—changing it from a system and method for increasing reliability through redundant routers to a system and method for increasing the security of the network through switch-level authentication. That is, the principle of operation of Li, using routers interchangeably to promote an uninterrupted flow of information, is changed completely, and in fact will not function at all, with the addition of a security protocol in which each communication received by a switch is authenticated according to an entity-specific protocol. The proposed modification of Li by Daley therefore cannot possibly support a prima facie case of obviousness. As such, the rejection of claims 1-53 should be withdrawn and the claims should be allowed.

### Does Not Teach or Suggest All of Applicants' Claim Limitations

To establish a prima facie case of obviousness under 35 U.S.C. § 103, the proposed combination of the cited references must teach or suggest all of Applicants' claim limitations. Independent claim 1 of the present invention claims, among other elements:

a processor for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said second switch and said third-type derivative of said pre-defined information about said second switch

Independent claim 10 of the present invention claims, among other elements, “sending a third-type derivative of said defined information concerning said first switch from said first port to said second port.” Independent claims 23, 37, and 50 contain similar elements. Independent claim 51 of the present invention claims, among other elements, “at said second switch, attempting to verify said first switches signature using said PKI public key uniquely associated with said second switch.”

In regard to claim 1, the Office Action, on page 7, paragraph 5, states that “Li teaches a system of routers that communicate through hello messages and include authentication messages (Col 3 lines 1-4, Col 10 line 65-Col 11 line 16).” The “system of routers that communicate through hello messages and include authentication messages” of Li does not disclose the

processor for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said second switch and said third-type derivative of said pre-defined information about said second switch

of claim 1 in the present application. The related method of Li does not disclose “sending a third-type derivative of said defined information concerning said first switch from said first port to said second port” as claimed in claim 10 of the present application or similarly claimed in claims 23, 37, and 50. Nor does the related method of Li disclose “at said second switch, attempting to verify said first switches signature using said PKI public key uniquely associated with said second switch” as claimed in claim 51 of the present application.

In regard to claim 1, the Office Action, on page 8, paragraph 5, states that “Daley teaches a strong authentication protocol . . . .” The “strong authentication protocol” of Daley does not disclose the

processor for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said second switch and said third-type derivative of said pre-defined information about said second switch

of claim 1 in the present application. The related method of Daley does not disclose “sending a third-type derivative of said defined information concerning said first switch from said first port to said second port” as claimed in claim 10 of the present application or similarly claimed in

claims 23, 37, and 50. Nor does the related method of Daley disclose “at said second switch, attempting to verify said first switches signature using said PKI public key uniquely associated with said second switch” as claimed in claim 51 of the present application.

Applicants respectfully submit that the Office Action cites references for elements which those references do not teach. Neither Li, nor Daley, nor any other reference cited in the Office Action has been shown by the Examiner to teach any of the claimed elements above. The combination of these references, therefore, cannot teach any of these claimed elements. Each dependent claim of the invention, depending directly or indirectly from one of the above independent claims, necessarily includes the limitations of the above claims. Thus, the Office Action has failed to establish a prima facie case of obviousness in any of claims 1-53. For this reason alone, the rejections under 35 USC 103(a) should be withdrawn, and the claims should be allowed.

#### No Prima Facie Case of Obviousness

As shown above, there is no suggestion or motivation to combine the references proposed in the Office Action, there is no reasonable expectation of success in the proposed combination of these references, and the proposed combination of the references does not teach or suggest all of Applicants’ claim limitations. As none of the three criteria for establishing a prima facie case of obviousness have been met, the Examiner has failed to meet his burden to establish a prima facie case of obviousness. MPEP § 2142. Applicants respectfully traverse each rejection, and request the withdrawal of the rejections and the allowance of claims 1-53.

#### Supplemental Amendment

This Supplemental Amendment repeats all of the arguments of the prior response filed on March 22, 2006 for convenience and corrects the listing of the claims by properly following 37 CFR 1.121 in amending claims.

\*\*\*\*\*

**CONCLUSION**

Reconsideration of the pending claims in light of the above remarks and allowance of all pending claims are respectfully requested. If, after considering this reply, the Examiner believes that a telephone conference would be beneficial towards advancing this case to allowance, the Examiner is invited to contact the undersigned attorney at the number listed.

**May 1, 2006**

Date

**/T. Austin Crone/**

T. Austin Crone

Reg. No. 56,335

Wong, Cabello, Lutsch, Rutherford & Brucculcri, L.L.P.

20333 State Highway 249, Suite 600

Houston, Texas 77070

Voice: 832-446-2407

Facsimile: 832-446-2424



## **Exhibit A**

**BEST AVAILABLE COPY**

**FIPS PUB 196**

**FEDERAL INFORMATION  
PROCESSING STANDARDS PUBLICATION**

**1997 February 18**

**U.S. DEPARTMENT OF COMMERCE / National Institute of Standards and Technology**

**ENTITY AUTHENTICATION  
USING  
PUBLIC KEY CRYPTOGRAPHY**

**CATEGORY: COMPUTER SECURITY  
SUBCATEGORY: ACCESS CONTROL**

U.S. DEPARTMENT OF COMMERCE, William M. Daley, *Secretary*  
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY,

**Foreword**

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996, and the Computer Security Act of 1987, Public Law 104-106. These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the Federal Government. The NIST, through its Information Technology Laboratory, provides leadership, technical guidance, and coordination of Government efforts in the development of standards and guidelines in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899.

Shukri Wakid, *Director*  
Information Technology Laboratory

**Abstract**

This standard specifies two challenge-response protocols by which entities in a computer system may authenticate their identities to one another. These may be used during session initiation, and at any other time that entity authentication is necessary. Depending on which protocol is implemented, either one or both entities involved may be authenticated. The defined protocols are derived from an international standard for entity authentication based on public key cryptography, which uses digital signatures and random number challenges.

Authentication based on public key cryptography has an advantage over many other authentication schemes because no secret information has to be shared by the entities involved in the exchange. A user (claimant) attempting to authenticate oneself must use a private key to digitally sign a random number challenge issued by the verifying entity. This random number is a time variant parameter which is unique to the authentication exchange. If the verifier can successfully verify the signed response using the claimant's public key, then the claimant has been successfully authenticated.

Key words: access control, authentication, challenge-response, computer security, cryptographic modules, cryptography, Federal Information Processing Standard (FIPS), telecommunications security.

# **Federal Information Processing Standards Publication 196**

**1997 February 18**

**ANNOUNCING**

## **ENTITY AUTHENTICATION USING PUBLIC KEY CRYPTOGRAPHY**

Federal Information Processing Standards (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996, and the Computer Security Act of 1987, Public Law 104-106.

- 1. Name of Standard.** Entity Authentication Using Public Key Cryptography (FIPS PUB 196).
- 2. Category of Standard.** Computer Security, Subcategory Access Control.
- 3. Explanation.** This standard specifies two challenge-response protocols by which entities in a computer system may authenticate their identities to one another. These protocols may be used during session initiation, and at any other time that entity authentication is necessary. Depending on which protocol is implemented, either one or both entities involved may be authenticated. The defined protocols are derived from an international standard for entity authentication based on public key cryptography, which uses digital signatures and random number challenges.

Authentication based on public key cryptography has an advantage over many other authentication schemes because no secret information has to be shared by the entities involved in the exchange. A user (claimant) attempting to authenticate oneself must use a private key to digitally sign a random number challenge issued by the verifying entity. This random number is a time variant parameter which is unique to the authentication exchange. If the verifier can successfully verify the signed response using the claimant's public key, then the claimant has been successfully authenticated.

- 4. Approving Authority.** Secretary of Commerce.
- 5. Maintenance Agency.** Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory.
- 6. Cross Index.**
  - a.** FIPS PUB 140-1, Security Requirements for Cryptographic Modules.



- b. FIPS PUB 171, Key Management Using ANSI X9.17.
- c. FIPS PUB 180-1, Secure Hash Standard.
- d. FIPS PUB 186, Digital Signature Standard.
- e. FIPS PUB 190, Guideline for the Use of Advanced Authentication Technology Alternatives.
- f. ANSI X9.17-1985, Financial Institution Key Management (Wholesale).
- g. ISO/IEC 9798-1:1991, Information technology - Security techniques - Entity authentication mechanisms - Part 1: General model.
- h. ISO/IEC 9798-3:1993, Information technology - Security techniques - Entity authentication mechanisms - Part 3: Entity authentication using a public key algorithm.

Other NIST publications may be applicable to the implementation and use of this standard. A list (NIST Publications List 91) of currently available computer security publications, including ordering information, can be obtained from NIST.

**7. Applicability.** This standard is applicable to all Federal departments and agencies that use public key based authentication systems to protect unclassified information within computer and digital telecommunications systems that are not subject to Section 2315 of Title 10, U.S. Code, or Section 3502(2) of Title 44, U.S. Code. This standard shall be used by all Federal departments and agencies in designing, acquiring and implementing public key based, challenge-response authentication systems at the application layer within computer and digital telecommunications systems. This includes all systems that Federal departments and agencies operate or that are operated for them under contract. In addition, this standard may be used at other layers within computer and digital telecommunications systems.

This standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it is either cost effective or provides interoperability for commercial and private organizations.

**8. Applications.** Numerous applications can benefit from the incorporation of entity authentication based on public key cryptography, when the implementation of such technology is considered cost-effective. Networking applications that require remote login will be able to authenticate clients who have not previously registered with the host, since secret material (e.g., a password) does not have to be exchanged beforehand. Also, point-to-point authentication can take place between users who are unknown to one another. The authentication protocols in this standard may be used in conjunction with other public key-based systems (e.g., a public key infrastructure that uses public key certificates) to enhance the security of a computer system.

**9. Specifications.** Federal Information Processing Standard (FIPS) 196, *Entity Authentication Using Public Key Cryptography* (affixed).

**10. Implementations.** The authentication protocols described in this standard may be implemented in software, firmware, hardware, or any combination thereof.

11. **Export Control.** Implementations of this standard are subject to Federal Government export controls as specified in Title 15, Code of Federal Regulations, Parts 768 through 799. Exporters are advised to contact the Department of Commerce, Bureau of Export Administration, for more information.

12. **Implementation Schedule.** This standard becomes effective April 6, 1997.

13. **Qualifications.** The authentication technology described in this standard is based upon information provided by sources within the Federal Government and private industry. Authentication systems are designed to protect against adversaries (e.g., hackers, organized crime, economic competitors) mounting cost-effective attacks on unclassified government or commercial data. The primary goal in designing an effective security system is to make the cost of any attack greater than the possible payoff.

While specifications in this standard are intended to maintain the security of an authentication protocol, conformance to this standard does not guarantee that a particular implementation is secure. It is the responsibility of the manufacturer to build the implementation of an authentication protocol in a secure manner. This standard will be reviewed every five years in order to assess its adequacy.

14. **Waivers.** Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency may re-delegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, U.S. Code. Waivers shall be granted only when:

- a. Compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or
- b. Cause a major adverse financial impact on the operator which is not offset by Government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive classified portions clearly identified, shall be sent to: National Institute of Standards and Technology, ATTN: FIPS Waiver Decisions, Building 225, Room A231, Gaithersburg, MD 20899.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C. Section 552(b), shall be part of the procurement documentation and retained by the agency.

**15. Where to Obtain Copies.** Copies of this publication are available for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 196 (FIPS PUB 196), and identify the title. When microfiche is desired, this should be specified. Payment may be made by check, money order, credit card, or deposit account.

Federal Information  
Processing Standards Publication 196

1997 February 18

Specifications for

ENTITY AUTHENTICATION  
USING PUBLIC KEY CRYPTOGRAPHY

CONTENTS

1.	INTRODUCTION .....	7
2.	GENERAL .....	8
2.1	Scope .....	8
2.1.1	Implementation Criteria .....	8
2.1.2	Overview .....	8
2.2	Threats .....	10
2.3	Definitions and notation .....	11
2.3.1	Definitions .....	11
2.3.2	Notation .....	12
3.	ENTITY AUTHENTICATION PROTOCOLS .....	14
3.1	Authentication protocol issues .....	14
3.1.1	Digital signatures .....	14
3.1.2	Random numbers .....	14
3.1.3	Identifiers .....	15
3.1.4	Public key certificates .....	15
3.1.5	Optional fields and steps .....	16
3.1.6	Authentication token encoding methods .....	17
3.2	Unilateral authentication protocol .....	18
3.3	Mutual authentication protocol .....	21
Appendix A	.....	26
A.1	Abstract Syntax Notation One (ASN.1) .....	26
A.2	ASN.1 Specification of Entity Authentication Tokens and Messages .....	27
A.3	ASN.1 Specification of Public-Key Certification Information .....	30
Appendix B	.....	33

B.1 ASN.1 Specification of SPKM Tokens and Messages .....	33
B.2 ASN.1 Specification of Public-Key Certification Information .....	37
Appendix C .....	38
C.1 Background .....	38
C.2 Token and Message Formats Based on ANSI X9.26 .....	38
C.2.1 Abbreviations .....	38
C.2.2 Notation .....	40
C.2.3 Basic Functions .....	40
C.2.4 Message Formats .....	41
Appendix D .....	44
D.1 Background .....	44
D.2 Base64 Content-Transfer-Encoding .....	45
D.3 Format of In-Band Authentication Messages .....	46
D.4 Error detection .....	47
D.5 Example .....	47
Appendix E .....	49

## 1. INTRODUCTION

This publication specifies two protocols for entity authentication that use a public key cryptographic algorithm for generating and verifying digital signatures. One entity can prove its identity to another entity by using a private key to generate a digital signature on a random challenge. The use of cryptography provides for strong authentication, which does not require authenticating entities to share secret information. Federal government computer systems which implement this standard shall generate and verify digital signatures in accordance with a FIPS approved public key digital signature algorithm (e.g., FIPS PUB 186, *Digital Signature Standard*).

International Standard ISO/IEC 9798-3:1993, *Entity authentication using a public key algorithm* (ISO/IEC 9798-3), serves as the basis for the authentication protocols defined in Section 3 below. That international standard defines five different protocols, addressing both unilateral and mutual entity authentication, that make use of a public key cryptographic algorithm. In particular, digital signatures are used in determining an entity's authenticity. Only one protocol for each unilateral and mutual authentication was selected from ISO/IEC 9798-3. Certain authentication token fields and protocol steps are described in greater detail in this standard than in ISO/IEC 9798-3.

Although ISO/IEC 9798-3 serves as the basis for this standard, this specification is less strict, in that it allows for the arbitrary ordering of token fields. This allowance therefore enables other non-ISO public key authentication protocols to meet the requirements of this standard. Those requirements are specified in the following sections.

Section 2 of this standard presents a general overview of the entity authentication protocols defined herein. It also (1) highlights the criteria that must be met to conform to this standard, (2) briefly describes threats addressed by using the authentication protocols, and (3) lists definitions and notation used in this standard. The authentication protocols, along with issues pertaining to authentication token information, are described in detail in Section 3. Several appendices accompanying this standard describe optional methods for formatting and encoding authentication information. These methods are included for informational purposes only, to help promote the interoperability of various implementations of the authentication protocols defined in Section 3.

## 2. GENERAL

### 2.1 Scope

#### 2.1.1 Implementation Criteria

To acceptably implement this standard, an implementation must meet the following criteria:

- 1) Each entity in an authentication exchange must use a FIPS approved digital signature algorithm to generate and/or verify digital signatures;
- 2) Each entity must generate (pseudo)random numbers using a FIPS approved (pseudo)random number generator;
- 3) Each entity acting as a claimant must be bound to a public/private key pair; the private key should remain in the sole control of the claimant who uses that key to sign a random challenge. The key binding requires a unique authentication identifier for each claimant, so that a verifier can distinguish between multiple claimants; and
- 4) One or both of the authentication protocols in this standard must be implemented. For each protocol, steps and token fields marked as [OPTIONAL] do not need to be implemented, except where indicated otherwise. However, all other steps and token fields must be implemented.

#### 2.1.2 Overview

Entity authentication protocols in this standard make use of a digital signature algorithm for the generation of authentication tokens. The authentication protocols are independent of the nature of the authenticating entities (e.g., for mutual authentication, the same protocol is used for human-human, human-process, and process-process authentication). In situations where a human is involved as a principal, a two-step sequence usually takes place, due to the complexity of cryptography. A human user first authenticates oneself to a cryptographic module, which then acts as a claimant and performs the actual signature generation and/or verification on behalf of the human user (see Section 3.1.1).

The authentication of an entity (viz., a claimant to a verifier) depends on two successful actions: (1) the verification of the claimant's binding with its public/private key pair, and (2) the verification of the claimant's digital signature on a random number challenge. A binding of an entity's unique identifier with its key pair is essential to proving the authenticity of that entity's identity. This must be done prior to any authentication exchange. During an authentication exchange, a random number challenge generated by the verifier is associated with the claimant's identifier. The claimant then generates a signature on that challenge, which is freshly generated for that particular exchange. In order to verify a signature, the verifier uses the claimant's identifier to find a public key that is bound to that identifier. If that public key can be used to

successfully verify the claimant's signature on the challenge, then the verifier has in fact verified that the claimant is the same entity that is bound to the key pair. This chain of associations, bindings, and signatures is what allows an entity to successfully authenticate itself. The next several paragraphs address some issues of entity-key bindings, random challenges, and identifiers.

Public key certificates are not required by this standard, and the utilization of a public key infrastructure lies outside the scope of this standard. Whether or not public key certificates are used in an authentication implementation, each public/private key pair shall be bound to a particular entity. Such a binding may be performed by a verifier or a third party that is trusted by the verifier. Trusted third parties may be used in conjunction with this standard to distribute delegation keys, login tickets, public keys, or public key certificates. Delegation keys are keys issued by one entity to let another entity act upon the issuer's behalf; login tickets are generated by a third party, and used by one entity to authenticate to another. Neither of these items is used in this standard, but may be included in a particular implementation using the optional text fields provided in the exchanged authentication tokens (see Section 3.1.5). Trusted third parties may provide other necessary services, such as a courier service to transport valid public keys.

Since the protocols defined in this standard utilize (pseudo)random number values for the authentication tokens' time variant parameters, authenticating entities do not have to use synchronized clocks to verify the freshness and timeliness of authentication tokens. (Note: Throughout the rest of this document, the term "random" number will imply the use of either a random or pseudorandom number.) Authentication exchanges using date-time stamps and sequence numbers were not chosen for this standard due to their requirements of maintaining synchronized clocks and sequence number log tables, respectively. Random number challenges are generally easier to use in widely distributed environments where entities do not necessarily know one another prior to authentication.

A naming convention for the entities involved in an authentication exchange is not defined in this standard. However, unique, distinguishing identifiers for participating authentication entities should be established prior to the execution of either of those protocols. Each entity being authenticated must have such an identifier, which can be used to uniquely associate it with a public/private key pair.

Biometric authentication techniques are not included in the authentication exchanges in Section 3. Information pertaining to biometrics, or the results of performing a biometric live scan, may be included in an authentication token's optional text field, and that data may be used in determining authentication success or failure. However, the lack of that biometric functionality, in an implementation of either protocol, will not prevent that implementation from meeting the requirements of this standard.

Upon completion of either of the entity authentication protocols in this standard, the entity performing the final verification step may send an acknowledgment of verification success or failure to the other entity involved in the exchange. Although the format and use of such an



acknowledgment is not within the scope of this standard, in certain implementations it may be necessary to inform the other principal of a(n) (un)successful authentication exchange.

## 2.2 Threats

The protocols defined in this document address several threats, including masquerade, password compromise, replay attacks, and the signing of pre-defined data. Using challenges and digital signatures eliminates the need for transmitting passwords for authentication, which reduces the threat of their compromise. Such a compromise would allow an attacker to use the same information to authenticate repeatedly. By using a private key to generate digital signatures for authentication, it becomes computationally infeasible for an attacker to masquerade as another entity. However, implementations may still rely on passwords for an entity to access its private key. In that case, passwords must be kept secure. Although the use of public key cryptography eliminates the need for entities to share a secret value, it is extremely important that each claimant always keeps its private key secure, and under its sole control.

The use of random number challenges also prevents an intruder from copying an authentication token signed by another user and replaying it successfully at a later time. However, a new random number challenge should be generated for each authentication exchange. The security of replay prevention also hinges on the generation of random number challenges which have a low probability of being repeated.

Finally, by including a random number of its own in an authentication token, a claimant can preclude the signing of only data that is pre-defined by the verifier. If a claimant uses a private key for more than just signing authentication tokens, for example, then a verifier could maliciously create a challenge consisting of information which is meaningful in another context. This can be prevented when the claimant signs both the challenge and unpredictable, meaningless data - a random number. This is why the responder in the mutual authentication protocol generates a signature over both random numbers, instead of just signing the initiator's random number challenge.

The authentication protocols in Section 3 do not address other threats, which include denial of service, session capture, transmission modification, and the use of another entity's compromised private key. No aspect of the authentication tokens or protocols preclude another entity from rerouting or modifying authentication transmissions. Maintaining the secrecy of one's private key is of utmost importance, and failure to do so may result in one entity masquerading as another entity by using the latter's private key for authentication. Other security measures, which lie outside the scope of this standard, may be needed in order to address such additional threats and vulnerabilities.

## 2.3 Definitions and notation

### 2.3.1 Definitions

Some of the following definitions are taken from terminology defined in ISO/IEC 9798-1:1991, *General Model* (ISO/IEC 9798-1) which describes the general model for the ISO/IEC 9798 series of entity authentication standards. Other definitions are from FIPS PUB 140-1, Section 2.1.

*Authentication token* (viz., *token*): authentication information conveyed during an authentication exchange.

*Binding*: an acknowledgment by a trusted third party that associates an entity's identity with its public key. This may take place through (1) a certification authority's generation of a public key certificate, (2) a security officer's verification of an entity's credentials and placement of the entity's public key and identifier in a secure database, or (3) an analogous method.

*Claimant*: an entity which is or represents a principal for the purposes of authentication, together with the functions involved in an authentication exchange on behalf of that entity. A claimant acting on behalf of a principal must include the functions necessary for engaging in an authentication exchange. (e.g., a smartcard (claimant) can act on behalf of a human user (principal))

*Cryptographic module*: the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. (See FIPS PUB 140-1)

*Digital signature* (viz., *signature*): a nonforgeable transformation of data that allows the proof of the source (with nonrepudiation) and the verification of the integrity of that data.

*Distinguishing identifier*: information which unambiguously distinguishes an entity in the authentication process.

*Entity*: any participant in an authentication exchange; such a participant may be human or non-human, and may take the role of a claimant and/or verifier.

*FIPS approved security method*: a security method (e.g., cryptographic algorithm, cryptographic key generation algorithm or key distribution technique, random number generator, authentication technique, or evaluation criteria) that is either a) specified in a FIPS, or b) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS.

*Initiator*: the entity that initiates an authentication exchange.

*Principal*: an entity whose identity can be authenticated.

*Private key:* a cryptographic key used with a public key cryptographic algorithm, which is uniquely associated with an entity, and not made public; it is used to generate a digital signature; this key is mathematically linked with a corresponding public key.

*Public key:* a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public; it is used to verify a digital signature; this key is mathematically linked with a corresponding private key.

*Public key certificate (certificate):* a set of data that unambiguously identifies an entity, contains the entity's public key, and is digitally signed by a trusted third party (certification authority).

*Public key infrastructure (PKI):* an architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys.

*Responder:* the entity that responds to the initiator of the authentication exchange.

*Signed data:* data on which a digital signature is generated.

*Unsigned data:* data included in an authentication token, in addition to a digital signature. An exception to this is TokenBA<sub>1</sub> in each authentication exchange, which contains only unsigned data and no signature. Unsigned data gives information to the token recipient which may be used to verify the token's signature and/or generate a response token. This unsigned data *may* be equivalent to the signed data, but not necessarily.

*Verifier:* an entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.

### 2.3.2 Notation

In Section 3, the following notation is used in describing parts of the authentication exchanges. Most of this notation is used in ISO/IEC 9798-3.

A - the distinguishing identifier (name) of entity A.

B - the distinguishing identifier (name) of entity B.

S<sub>X</sub> - a private key associated with entity X, used in generating a digital signature.

R<sub>X</sub> - a random number issued by entity X.

X || Y - the result of the concatenation of data items X and Y, not necessarily in that order.

CertX - a trusted third party's certificate for entity X, that binds X with a public-private key pair; may also indicate a chain of certificates beginning or ending with CertX.

TextN - data of unspecified format or length that may be included in a token.

TokenID - token identifier - information accompanying an authentication token that may be used to identify the token and/or protocol type to assist token processing by the recipient.

TokenXY - a token sent from entity X to entity Y.

TokenXY<sub>i</sub> - the i<sup>th</sup> token sent from entity X to entity Y.

sS<sub>X</sub>(Z) - the digital signature of data Z using the private key S ; Z is referred to as "signed data".

[ Z ] - indicates that item Z is an optional element.

[OPTIONAL] - indicates that the accompanying step is optional; it does not have to be executed in order for the implementation to conform to this standard.

### 3. ENTITY AUTHENTICATION PROTOCOLS

#### 3.1 Authentication protocol issues

Certain factors should be considered before initiating either of the authentication protocols described in this standard.

##### 3.1.1 Digital signatures

Each entity involved in an authentication protocol in Section 3 must have the ability to generate and/or verify a digital signature. Entities acting as claimants must have a digital signature generation capability, and verifiers must have a digital signature verification capability. A FIPS approved public key digital signature algorithm (e.g., FIPS PUB 186, *Digital Signature Standard (DSS)*) must be implemented to provide these digital signature functions.

A public/private key pair compliant with the digital signature algorithm must be possessed by each claimant. *It is critical to the security of the authentication exchanges that a private key remain accessible to only one claimant.* The entity authentication implementation shall employ an identity-based operator authentication mechanism "in order to verify the authorization of the operator to assume the desired roles and to request corresponding services" (FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*). This establishes a one-to-one relationship between an entity and the private (signing) key, and it also helps prevent unauthorized entities from authenticating themselves falsely using the key material.

##### 3.1.2 Random numbers

To create random numbers for the two authentication exchanges described in this standard, only FIPS approved random number generators shall be used. At a minimum, these include generators found in:

- Appendix 3 of FIPS PUB 186, and
- Appendix C of ANSI X9.17-1985, Financial Institution Key Management (Wholesale).

In the authentication exchanges described in Sections 3.2 and 3.3, the verifier uses a random number as a challenge to the claimant, and the claimant uses a random number to preclude signing only data determined by the verifier (see Section 2.2 for a discussion of potential threats).

An implementor may choose to use other types of time variant parameters in the authentication exchanges in this standard, *however* they shall be used in conjunction with the random number challenge, which remains the basis for verifying an entity's authenticity. One possible approach is to combine (e.g., exclusive-OR, concatenate, etc.) a non-repeating sequence number with the output of the random number generator, and using the result as the random number challenge.

It is important to note that each entity that acts as a verifier must maintain state, because knowledge of the original random number challenge is essential when the verifier attempts to

verify the claimant's response. To maintain state for the duration of an authentication exchange, a verifier must keep a record of both (1) a freshly generated random number challenge and (2) an association between that challenge and the claimant. Linking the claimant to the appropriate random number challenge is *especially* important when the verifier is involved in several simultaneous authentication sessions. How this is done depends on the particular implementation. In some implementations, it may be necessary to link the random number with the claimant using the optional TokenID field which may be sent with a token.

### 3.1.3 Identifiers

Unique, distinguishing identifiers shall be determined for all entities which have the potential for communicating with one another, before the authentication protocol is initiated. A naming convention shall be established such that a verifier can differentiate between all entities which act as claimants, and each claimant has a unique identifier for each verifier. If certificates are used, the naming convention used in identifying entities to one another during the authentication exchange does not have to be the same as the certificate naming convention. However, each entity must have some means of correlating a name in a certificate with the identifier used during authentication.

In the entity authentication protocols below, a token identifier (TokenID) may be included with each token transmission. Such an identifier might indicate the type of token being sent, and the authentication exchange to which it belongs. The format for these token identifiers is outside the scope of this standard.

### 3.1.4 Public key certificates

If public key certificates are used in the authentication process, then they must be generated prior to the authentication exchange, and should be maintained so that they are readily accessible to any entity that wishes to authenticate another entity's identity. Typically, a certificate is generated by a trusted third party and then either distributed or stored where prospective authenticating entities have access to it. When an entity wishes to obtain a certificate for verification purposes, the certificate may be retrieved from a directory service, a local cache, or an authentication message. If certificates are retrieved from a directory service or a local cache, it is most expedient to do this prior to the authentication exchange. During an authentication exchange, the entity generating the token may send its certificate or a chain of certificates with the token. Certificate formats are outside the scope of this standard, but particular formats may be recommended or mandated by other FIPS, NIST Special Publications, or other Federal regulations.

The manner in which a certificate or certificate chain is verified depends on the configuration of the public key infrastructure in use. Generally speaking, however, to verify the binding between the claimant and its public key, a verifier must have a chain of valid, verifiable certificates - from the claimant's certificate to a certificate issued by a trusted third party whose public key is known to the verifier. The manner in which the certificate chain is retrieved is outside the scope of this

standard. Failure of any verification in the certificate chain shall result in a failure to verify the signature on the claimant's certificate.

If certificates are not used, then the claimant must be bound to its public/private key pair in some other manner. The claimant's public key and any global variables necessary for signature verification may be exchanged prior to initiating the authentication exchange. A trusted third party may be used by a verifier to obtain a claimant's public key. Each entity which performs authentication verifications may choose to maintain a public key database. The method by which these tasks are accomplished is outside the scope of this standard.

### 3.1.5 Optional fields and steps

Each of the messages exchanged in the authentication protocols include fields that are marked "[OPTIONAL]", as are some steps in the protocols. Neither those fields nor steps have to be implemented in order to conform to this standard, unless indicated otherwise. The authentication of each claimant does not depend on the use of any optional fields or steps. It is left up to the implementor to determine which optional fields and steps will be implemented, and how they will be used.

Each of the tokens exchanged in both the unilateral and mutual protocols contain generic "Text" fields. These fields are optional and have a format which is implementation-specific. The optional text field in each authentication token represents an aggregation of optional fields, which can appear in any order throughout the token.

Each authentication token includes an optional text field(s) containing data that does not have to be signed. Note that data integrity is *not* guaranteed for information which is included in the unsigned portion of a token but which is *not* digitally signed (i.e., unsigned data that is not included in the signed data). It is recommended, but not required, that a signature be generated over *all* information included in a token. The type of data that may be included is determined by the implementor, and is not limited by the specifications in this standard. The number of different types of data in each optional field is not limited, either. Use of the text fields should be carefully implemented, because their use *may* - depending on the implementation - create vulnerabilities in the authentication exchange. Some possible uses of the text fields are listed below:

Identifiers - An entity may choose to include an identifier for itself in the text field of a token. If certificates are not used to distribute a claimant's public key, then the implementation may require that the claimant include information identifying itself in the authentication token.

Time value - Another time variant parameter may be included in a token's text field, in addition to the random challenges that are used to determine the authenticity of entities. *However, this additional value shall not replace the random number value as the verifier's challenge to the claimant.* For example, a time value may be included in a token for access control auditing, if tokens are logged by a verifier upon successful completion of an authentication exchange.

Key exchange data - Text fields may include information used to distribute a cryptographic key (or keys). For example, an encrypted session key, or information used in establishing a session key may be included in the text field. How the key distribution is performed is not specified in or required by this standard. When either of the protocols in this standard is used to establish a key, that key shall not be used until each claimant in the exchange has been successfully authenticated.

Biometric data - An implementation, in addition to requiring a verifiable response to a random challenge, may optionally include biometric authentication data to determine an entity's authenticity. This is a physical characteristic of a claimant (or the principal on whose behalf the claimant is acting), which is an additional factor of authentication. See FIPS PUB 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, for more information.

### 3.1.6 Authentication token encoding methods

Descriptions of the authentication protocols in Sections 3.2 and 3.3 specify the contents of authentication tokens and steps for token generation and verification. However, the formatting and encoding of these tokens is not specified in this standard, and they are left to the discretion of the implementor. The interoperability of different implementations of the authentication protocols will rely, to some extent, on how tokens and messages are formatted and encoded. This is especially important since token fields are ordered arbitrarily, and the format and content of optional text fields are not specified. To provide some implementation guidance, several informative appendices (A, B, C, and D) are provided in this standard which specify optional examples of formatting and encoding methods. The implementation of any one of those methods is *not* required for meeting the specifications of this standard.



### 3.2 Unilateral authentication protocol

The following unilateral entity authentication protocol is based on Section 5.1.2, "Two pass authentication", of ISO/IEC 9798-3. Certain authentication token fields and protocol steps are specified in greater detail in this section than in ISO/IEC 9798-3. The verifier may choose to terminate the authentication exchange at any time. Figure 1 illustrates this exchange.

The unilateral authentication protocol begins with the verifier (B) challenging the claimant (A). The description below allows for situations where the claimant may be the initiator of the exchange, depending on the application of this protocol.

It is important to note that the success of an entity's authentication, according to this standard, is not dependent on the information contained in the text fields. As described in Section 2.1, the authentication of an entity depends on two things: (1) the verification of the claimant's binding with its key pair, and (2) the verification of the claimant's digital signature on the random number challenge. How text field information is used is beyond the scope of this standard.

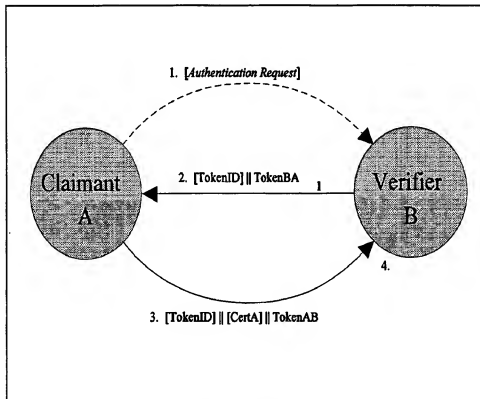


Figure 1 Unilateral Authentication Protocol

Unilateral entity authentication occurs as follows:

- 1) [OPTIONAL] The claimant, A, selects the verifier, B, to which it will authenticate, and makes an authentication request to B - the format of this request is not defined in this standard.
- 2) The verifier, B, determines if it will continue, initiate, or terminate the authentication exchange. If it attempts to authenticate the claimant, the verifier then
  - a) generates a random number challenge, which is the value for the  $R_B$  field in  $TokenBA_1$  below, and retains this value.
  - b) [OPTIONAL] generates and/or selects other data which is to be included in the Text1 field of  $TokenBA_1$ .

The verifier creates a challenge token of the following form:

$$TokenBA_1 = R_B \parallel [Text1]$$

Entity B sends a message consisting of  $TokenBA_1$  and an optional TokenID to the claimant. The message from the verifier to the claimant is of the form:

$$[TokenID] \parallel TokenBA_1$$

- 3) Upon receiving the message including  $TokenBA_1$ , the claimant, A,
  - a) [OPTIONAL] uses TokenID to determine which token is being received.
  - b) [OPTIONAL] retrieves information from the Text1 field, using it in a manner which is outside the scope of this standard.
  - c) generates a random number challenge, which is the value for the  $R_A$  field in  $TokenAB$  below.
  - d) [OPTIONAL] selects an identifier for the verifier, and includes that in the B field of  $TokenAB$ .
  - e) [OPTIONAL] generates and/or selects other data which is to be included in the Text2 and Text3 fields. In  $TokenAB$ , Text2 is a subset of the Text3 field, including cases where Text2 is the NULL set, and where Text2 equals Text3.

The claimant creates an authentication token, TokenAB, by concatenating data and generating a digital signature:

$$\text{TokenAB} = R_A \parallel [R_B] \parallel [B] \parallel [\text{Text3}] \parallel \text{sS} (R_A \parallel R_B \parallel [B] \parallel [\text{Text2}])$$

The signed data that are marked as optional are present only when their corresponding values are present in the unsigned part of TokenAB. Although  $R_B$  does not have to be in the unsigned data of TokenAB, it *must* be included in the signed data.

In addition to containing TokenAB, the message may optionally include a token identifier, TokenID, and the claimant's certificate (or chain of certificates), CertA. The message from the claimant to the verifier is of the form:

$$[\text{TokenID}] \parallel [\text{CertA}] \parallel \text{TokenAB}$$

- 4) Upon receiving the message including TokenAB, the verifier, B,
  - a) [OPTIONAL] uses TokenID to determine which token is being received.
  - b) verifies that the value of  $R_B$  is the same as the value retained in step 2)a), given that  $R_B$  is present in the unsigned part of TokenAB. If this value is *not* present, then the value retained in step 2)a) is used in the signature verification process in step 4)c).
  - c) verifies that the identifier for the claimant has been obtained in one of three ways: in CertA, TokenAB, or the authentication request in step 1), depending on which optional information has been included. In the event that certificates are not used for signature verification, then the identifier for entity A should be used to retrieve the claimant's public key in some unspecified manner; continue with step 4)e).
  - d) verifies the claimant's certificate or certificate chain, assuming certificates are used (see Section 3.1.4).
  - e) verifies the claimant's signature in TokenAB.
  - f) [OPTIONAL] retrieves data from the B, Text2, and Text3 fields, using them in a manner which is outside the scope of this standard.

Successful completion of parts b) through e) in step 4) means that the claimant, A, has authenticated itself to the verifier, B. If any of the verifications in parts b) through e) fail, then the authentication exchange is terminated. If certain conditions either are or are not met in the optional parts a) and f), the verifier may choose to terminate the authentication exchange; these conditions are implementation-specific, and outside the scope of this standard.

### 3.3 Mutual authentication protocol

The following mutual entity authentication protocol is based on Section 5.2.2, "Three pass authentication", of ISO/IEC 9798-3. Certain authentication token fields and protocol steps are specified in greater detail in this section than in ISO/IEC 9798-3. Either entity may choose to terminate the authentication exchange at any time. Figure 2 illustrates this exchange.

The mutual authentication protocol refers to entities A and B as "initiator" and "responder". This differs from terminology used to describe unilateral authentication in Section 3.2, because each entity acts as *both* a claimant and a verifier in the protocol below.

It is important to note that the success of an entity's authentication, according to this standard, is not dependent on the information contained in the text fields. As described in Section 2.1, the authentication of an entity depends on two things: (1) the verification of the claimant's binding with its key pair, and (2) the verification of the claimant's digital signature on the random number challenge. How text field information is used once an entity's authenticity is verified is beyond the scope of this standard.

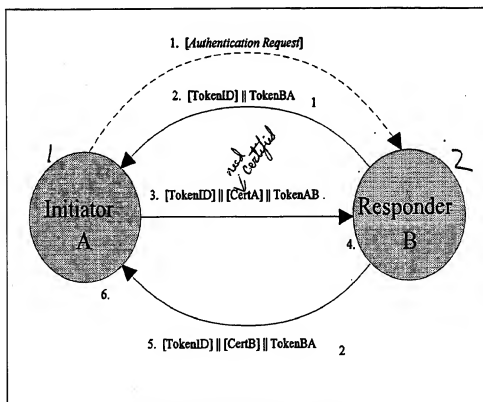


Figure 2 Mutual Authentication Protocol

Mutual entity authentication occurs as follows:

- 1) [OPTIONAL] The initiator, A, selects the responder, B, with which it will mutually authenticate, and makes an authentication request to B - the format of this request is not defined in this standard.
- 2) The responder, B, determines if it will continue, initiate, or terminate the authentication exchange. If it attempts to authenticate the initiator, the responder then
  - a) generates a random number challenge, which is the value for the  $R_B$  field in  $\text{TokenBA}_1$  below, and retains this value.
  - b) [OPTIONAL] generates and/or selects other data which is to be included in the Text1 field of  $\text{TokenBA}_1$ .

The responder creates a challenge token of the following form:

$\text{TokenBA}_1 = R_B \parallel [\text{Text1}]$

Entity B sends a message consisting of  $\text{TokenBA}_1$  and an optional  $\text{TokenID}$  to the initiator. The message from the responder to the initiator is of the form:

$[\text{TokenID}] \parallel \text{TokenBA}_1$

- 3) Upon receiving the message including  $\text{TokenBA}_1$ , the initiator, A,
  - a) [OPTIONAL] uses  $\text{TokenID}$  to determine which token is being received.
  - b) [OPTIONAL] retrieves information from the Text1 field, using it in a manner which is outside the scope of this standard.
  - c) generates a random number challenge which is the value for the  $R_A$  field in  $\text{TokenAB}$  below; the value of  $R_A$  is retained by the initiator.
  - d) [OPTIONAL] selects an identifier for the responder, and includes that in the B field of  $\text{TokenAB}$ .
  - e) [OPTIONAL] generates and/or selects other data which is to be included in the Text2 and Text3 fields. In  $\text{TokenAB}$ , Text2 is a subset of the Text3 field, including cases where Text2 is the NULL set, and where Text2 equals Text3.

The initiator creates an authentication token, TokenAB, by concatenating data and generating a digital signature:

$$\text{TokenAB} = R_A \parallel [R_B] \parallel [B] \parallel [\text{Text3}] \parallel s_{S_A}(R_A \parallel R_B \parallel [B] \parallel [\text{Text2}])$$

The signed data that are marked as optional are present only when their corresponding values are present in the unsigned part of TokenAB. Although  $R_B$  does not have to be in the unsigned data of TokenAB, it *must* be included in the signed data (see Section 2.2).

In addition to containing TokenAB, the message may optionally include a token identifier, TokenID, and the initiator's certificate (or chain of certificates), CertA. The message from the initiator to the responder is of the form:

$$[\text{TokenID}] \parallel [\text{CertA}] \parallel \text{TokenAB}$$

4) Upon receiving the TokenAB transmission, the responder, B,

- a) [OPTIONAL] uses TokenID to determine which token is being received.
- b) verifies that the value of  $R_B$  is the same as the value retained in step 2)a), given that  $R_B$  is present in the unsigned part of TokenAB. If this value is *not* present, then the value retained in step 2)a) is used in the signature verification process in step 4)e).
- c) verifies that the identifier for the initiator has been obtained in one of three ways: in CertA, TokenAB, or the authentication request in step 1), depending on which optional information has been included. In the event that certificates are not used for signature verification, then the identifier for entity A should be used to retrieve the initiator's public key in some unspecified manner; continue with step 4)e).
- d) verifies the initiator's certificate or certificate chain, assuming certificates are used (see Section 3.1.4).
- e) verifies the initiator's signature in TokenAB. ✓
- f) [OPTIONAL] retrieves data from the B, Text2, and Text3 fields, using them in a manner which is outside the scope of this standard.

Successful completion of parts b) through e) in step 4) means that the initiator, A, has authenticated itself to the responder, B. If any of the verifications in parts b) through e) fail, then the authentication exchange is terminated. If certain conditions either are or are not met in the optional parts a) and f), the responder may choose to terminate the authentication exchange; these conditions are implementation-specific, and outside the scope of this standard.

5) The responder, B,

- a) [OPTIONAL] selects an identifier for the initiator, and includes that in the A field of TokenBA<sub>2</sub> below.
- b) [OPTIONAL] generates and/or selects other data which is to be included in the Text4 and Text5 fields. In TokenBA<sub>2</sub>, Text4 is a subset of the Text5 field - this includes cases where Text4 is the NULL set, and where Text4 equals Text5.

The responder creates an authentication token, TokenBA<sub>2</sub>, by concatenating data and generating a digital signature:

$$\text{TokenBA}_2 = [R_B] \parallel [R_A] \parallel [A] \parallel [\text{Text5}] \parallel \text{sS}_B( R_B \parallel R_A \parallel [A] \parallel [\text{Text4}] )$$

The signed data that are marked as optional are present only when their corresponding values are present in the unsigned part of TokenBA<sub>2</sub>. Although R<sub>A</sub> and R<sub>B</sub> do not have to be in the unsigned data of TokenBA<sub>2</sub>, they *must* be included in the signed data (see Section 2.2).

In addition to containing TokenBA<sub>2</sub>, the message may optionally include a token identifier, TokenID, and the responder's certificate (or chain of certificates), CertB. The message from the responder to the initiator is of the form:

$$[\text{TokenID}] \parallel [\text{CertB}] \parallel \text{TokenBA}_2$$

6) Upon receiving the message including TokenBA<sub>2</sub>, the initiator, A,

- a) [OPTIONAL] uses TokenID to determine which token is being received.
- b) verifies that the value of R<sub>A</sub> is the same as the value retained in step 3)c), given that R<sub>A</sub> is present in TokenBA<sub>2</sub>. If this value is *not* present, then the value retained in step 3)c) is used in the signature verification process in step 6)f).
- c) verifies that the value of R<sub>B</sub> is the same value as the R<sub>B</sub> field retrieved from TokenBA<sub>1</sub>, given that R<sub>B</sub> is present in TokenBA<sub>2</sub>. If this value is not present, then the value of R<sub>B</sub> retrieved from TokenBA<sub>1</sub> is used in the signature verification process in step 6)f).
- d) verifies that the identifier for the responder has been obtained in one of three ways: in CertB, TokenBA<sub>2</sub>, or TokenBA<sub>1</sub>, depending on which optional information has been included. In the event that certificates are not used for signature verification, then the identifier for entity B should be used to retrieve the initiator's public key in some unspecified manner; continue with step 6)f).

- e) verifies the responder's certificate or certificate chain, assuming certificates are used (see Section 3.1.4).
- f) verifies the responder's signature on TokenBA<sub>2</sub>.
- g) [OPTIONAL] retrieves data from the A, Text4, and Text5 fields, using them in a manner which is outside the scope of this standard.

Successful completion of parts b) through f) in step 6) means that the responder, B, has authenticated itself to the initiator, A, and thus the entities have successfully mutually authenticated. If any of the verifications in parts b) through f) fail, then the authentication exchange is terminated. If certain conditions either are or are not met in the optional parts a) and g), the initiator may choose to terminate the authentication exchange - these conditions are implementation-specific, and outside the scope of this standard.



## Appendix A

### Example Authentication Tokens Using ASN.1 Notation and CER/DER Encoding

This appendix is provided for informational purposes only, and is not part of this standard. The purpose of this appendix is to provide implementors of this standard with an optional set of rules for formatting and encoding authentication tokens and messages from Section 3 of this standard. Abstract Syntax Notation One (ASN.1) is used to format authentication tokens and messages, which are then encoded using Canonical Encoding Rules (CER) or Distinguished Encoding Rules (DER). This appendix also specifies optional representations of other data such as public key certificates. The implementation of a unique set of encoding rules is necessary for interoperability to take place between various authentication domains.

The reader should note that in ASN.1 notation, optional fields are indicated with the word "OPTIONAL", and not with square brackets "[ ]", as used in the body of this standard. In ASN.1 notation, square brackets are used to indicate tagged fields.

#### A.1 Abstract Syntax Notation One (ASN.1)

This example definition is specified using the Abstract Syntax Notation One (ASN.1). ASN.1 is an international standard used by ISO and ITU (previously CCITT) protocols as well as many Internet protocols. It is comprised of two parts: the ASN.1 notation [1-4] and the ASN.1 encoding rules [5].

The *ASN.1 notation* is an abstract specification language used to describe the local representation of data. It allows the description of the complex data types carried in protocol messages, without concern for the underlying binary representation.

The *ASN.1 encoding rules* go hand-in-hand with the ASN.1 notation. Whereas the ASN.1 notation provides an abstract specification of the local representation of data, the ASN.1 encoding rules define the external representation of the data. In order to correctly interpret the binary-pattern representation of a data value, it is necessary to know (usually from the context), the type of the value being represented, as well as the encoding mechanism used to convert the value from its local representation to its external representation. The ASN.1 encoding rules define "tags" that are added to a data value to indicate the data type and length representation. The encoding rules also define the actual bit representation of the data value.

There may be more than one set of encoding rules that can be applied to data values that are defined using the ASN.1 notation. The ASN.1 encoding rules standard defines three sets of encoding rules, namely: basic encoding rules, canonical encoding rules, and distinguished encoding rules. Whereas the basic encoding rules give the sender of an encoding various choices as to how data values may be encoded, the canonical and distinguished encoding rules select just

one encoding from those allowed by the basic encoding rules, allowing the receiver to unambiguously decode the ASN.1 notation. The use of canonical or distinguished encodings is essential with protocol messages containing digitally signed data values, so that the receiver can verify the digital signature over the same exact data representation used by the sender to generate the signature.

The canonical and distinguished encoding rules differ from each other in the set of restrictions they place on the basic encoding rules. The distinguished encoding rules are more suitable if the encoded value is small enough to fit into the available memory and there is a need to rapidly skip over some nested values. The canonical encoding rules are more suitable if there is a need to encode values that are so large that they cannot readily fit into the available memory or it is necessary to encode and transmit part of a value before the entire value is available.

## A.2 ASN.1 Specification of Entity Authentication Tokens and Messages

Each protocol message is potentially comprised of three components, an optional token identifier, optional public-key certification data, and an authentication token.

MessageBA<sub>1</sub> is used in the unilateral authentication exchange and is sent by the verifier to the claimant. MessageBA<sub>1</sub> is also used in the mutual authentication exchange and is sent by the responder to the initiator. MessageBA<sub>1</sub> contains an optional token identifier and authentication token BA<sub>1</sub>.

```

- tokenId.tokenType = 0x0001 for unilateral authentication
- tokenId.tokenType = 0x0011 for mutual authentication

MessageBA1 ::= SEQUENCE {
    tokenId          [0]  TokenId OPTIONAL,
    tokenBA1        TokenBA1
}

TokenBA1 ::= SEQUENCE {
    ranB             RandomNumber,
    text1            Text OPTIONAL
}

```

MessageAB is used in the unilateral authentication exchange and is sent by the claimant to the verifier. MessageAB is also used in the mutual authentication exchange and is sent by the initiator to the responder. MessageAB contains an optional token identifier, optional certification information, and authentication token AB.

```

- tokenId.tokenType = 0x0002 for unilateral authentication
- tokenId.tokenType = 0x0012 for mutual authentication

```

```

MessageAB ::= SEQUENCE {
    tokenId          [0] TokenId OPTIONAL,
    certA            [1] CertData OPTIONAL,
    tokenAB
}

TokenAB ::= SEQUENCE {
    ranA             RandomNumber,
    ranB             RandomNumber OPTIONAL,
    entityB          EntityName OPTIONAL,
    text3            Text OPTIONAL,
    signature        SIGNATURE { SigDataAB }
}

-- if entityB is included in TokenAB, then it shall also be included in SigDataAB

SigDataAB ::= SEQUENCE {
    ranA             RandomNumber,
    ranB             RandomNumber,
    entityB          EntityName OPTIONAL,
    text2            Text OPTIONAL -- subset of text3
}

```

MessageBA<sub>1</sub> is used in the mutual authentication exchange and is sent by the responder to the initiator. MessageBA<sub>1</sub> contains an optional token identifier, optional certification information, and authentication token BA<sub>1</sub>.

```

-- tokenId.tokenType = 0x0013

MessageBA1 ::= SEQUENCE {
    tokenId          [0] TokenId OPTIONAL,
    certB            [1] CertData OPTIONAL,
    tokenBA1
}

TokenBA1 ::= SEQUENCE {
    ranB             [0] RandomNumber OPTIONAL,
    ranA             [1] RandomNumber OPTIONAL,
    entityA          EntityName OPTIONAL,
    text5            Text OPTIONAL,
    signature        SIGNATURE { SigDataBA1 }
}

-- if entityA is included in TokenBA1, then it shall also be included in SigDataBA1

SigDataBA1 ::= SEQUENCE {
    ranB             RandomNumber,
    ranA             RandomNumber,
    entityA          EntityName OPTIONAL,
    text4            Text OPTIONAL -- subset of text5
}

```

The token identifier is defined here to include the type of token and the protocol version number. This version is defined here as Version 2, to distinguish it from Version 1, which was defined in an earlier draft of this appendix.

```

TokenId ::= SEQUENCE {
    tokenType          INTEGER,
    protoVerNo         INTEGER {v2(2)},
}

```

The certification data includes a certification path and/or a certificate revocation list. The definitions for **CertificationPath** and **CertificateList** are imported from ITU-T Rec. X.509 | ISO/IEC 9594-8, The Directory: Authentication Framework [6], and are given below in Section A.3.

```

CertData ::= SEQUENCE {
    certPath           [0] CertificationPath OPTIONAL,
    certRevList        [1] CertificateList OPTIONAL
}
-- at least one of the components above shall be present

```

A random number is simply defined as an octet string.

```

RandomNumber ::= OCTET STRING

```

An entity name is defined as the alternative name forms defined in Draft Amendment 1 to ITU-T Rec. X.509 | ISO/IEC 9594-8 on Certificate Extensions [7].

```

EntityName ::= AltNames

AltNames ::= SEQUENCE OF CHOICE {
    otherName          [0] INSTANCE OF OTHER-NAME,
    rfc822Name         [1] IA5String,
    dNSName            [2] IA5String,
    x400Address        [3] ORAddress,
    directoryName      [4] Name,
    ediPartyName       [5] IA5String
}

OTHER-NAME ::= TYPE-IDENTIFIER

```

Text contains undetermined data which may be included at the discretion of a specific implementation of this standard. Therefore, it is defined here to simply be a bit string. The text data used in a specific implementation shall be defined and encoded using ASN.1 or some other data representation. In either case, the resulting data shall be unambiguously encoded (e.g., using ASN.1 distinguished or canonical encoding rules) and shall be represented here as a bit string.

```

Text ::= BIT STRING -- contains encoded text data

```

### A.3 ASN.1 Specification of Public-Key Certification Information

The definitions for **CertificatePath** and **CertificateList** are taken from Annex A of ITU-T Rec. X.509 | ISO/IEC 9594-8, The Directory: Authentication Framework [6]. These definitions describe Version 2 certificates and certificate revocation lists. Version 3 certificate extensions can be found in Draft Amendment 1 to ITU-T Rec. X.509 | ISO/IEC 9594-8 on Certificate Extensions [7].

- types -

```

CertificatePath ::= SEQUENCE {
    userCertificate      Certificate,
    theCACertificates    SEQUENCE OF CertificatePair OPTIONAL
}

CertificateList ::= SIGNED { SEQUENCE {
    signature            AlgorithmIdentifier,
    issuer               Name,
    lastUpdate           UTCTime,
    revokedCertificates  SIGNED { SEQUENCE OF SEQUENCE {
        signature        AlgorithmIdentifier,
        issuer           Name,
        userCertificate   CertificateSerialNumber,
        revocationDate   UTCTime
    }} OPTIONAL
}}

CertificatePair ::= SEQUENCE {
    forward [0] Certificate OPTIONAL,
    reverse [1] Certificate OPTIONAL
}
- at least one of the pair shall be present

Certificate ::= SIGNED { SEQUENCE {
    version [0] Version DEFAULT v1,
    serialNumber CertificateSerialNumber,
    signature AlgorithmIdentifier,
    issuer Name,
    validity Validity,
    subject Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueIdentifier [1] IMPLICIT UniqueIdentifier OPTIONAL,
    - if present, version must be v2
    subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL,
    - if present, version must be v2
}}

Version ::= INTEGER {v1(0), v2(1)}

CertificateSerialNumber ::= INTEGER

AlgorithmIdentifier ::= SEQUENCE {
    algorithm ALGORITHM.&id({SupportedAlgorithms}),
    parameters ALGORITHM.&type({SupportedAlgorithms}){@algorithm}
    OPTIONAL
}

```

- Definition of the following information object set is deferred, perhaps to standardized

- profiles or to protocol implementation conformance statements. The set is required to  
 - specify a table constraint on the parameters component of AlgorithmIdentifier.  
 - SupportedAlgorithms      ALGORITHM ::= { ... | ... }

```
Validity ::= SEQUENCE {
    notBefore      UTCTime,
    notAfter       UTCTime
}
```

```
SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm      AlgorithmIdentifier,
    subjectPublicKey BIT STRING
}
```

- information object classes -

ALGORITHM ::= TYPE-IDENTIFIER

- parameterized types -

```
SIGNED { ToBeSigned } ::= SEQUENCE {
    ToBeSigned,
    COMPONENTS OF SIGNATURE{ToBeSigned}
}
```

```
SIGNATURE { OfSignature } ::= SEQUENCE {
    AlgorithmIdentifier,
    ENCRYPTED { HASHED { OfSignature } }
}
```

```
ENCRYPTED { ToBeEnciphered } ::= BIT STRING ( CONSTRAINED BY {
    - must be the result of applying an encipherment procedure -
    - to the BER-encoded octets of a value of - ToBeEnciphered
})
```

```
HASHED { ToBeHashed } ::= OCTET STRING ( CONSTRAINED BY {
    - must be the result of applying a hashing procedure to the -
    - DER-encoded octets of a value of - ToBeHashed
})
```

The definition for UniqueIdentifier is imported from Annex A of ITU-T X.520 | ISO/IEC 9594-6, The Directory: Selected Attribute Types [8].

UniqueIdentifier ::= BIT STRING

The definition for Name is taken from Annex B of ITU-T Rec. X.501 | ISO/IEC 9594-2, The Directory: The Models [9].

- naming data types -

Name ::= CHOICE { RDNSequence - one possibility for now - }

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET SIZE(1 .. MAX) OF AttributeTypeAndValue

*- attribute data types -*

```
AttributeTypeAndValue ::= SEQUENCE{
    type      AttributeType({SupportedAttributes}),
    value      AttributeValue({SupportedAttributes}){@type}
}
```

AttributeType ::= ATTRIBUTE.&id

AttributeValue ::= ATTRIBUTE.&Type

*- Definition of the following information object set is deferred, perhaps to standardized  
- profiles or to protocol implementation conformance statements. The set is required to  
- specify a table constraint on the value component of AttributeTypeAndValue.*

*- SupportedAttributes*      ATTRIBUTE ::= { ... | ... }

The reader should consult Annex B of ITU-T Rec. X.501 | ISO/IEC 9594-2 [9] for the  
ATTRIBUTE information object class specification.

---

## Appendix B

### Example Authentication Token Formatting and Encoding Based on the Simple Public-Key GSS-API Mechanism (SPKM) Specification

This appendix is provided for informational purposes only, and is not part of this standard. The purpose of this appendix is to provide implementors of this standard with an optional method for formatting and encoding authentication tokens in Section 3 of this standard.

The Simple Public-Key GSS-API Mechanism (SPKM) Specification is an Internet Proposed Standard (RFC 2025) [10] that describes several challenge-response mechanisms to enable entity authentication using public-key cryptography. That specification "defines protocols, procedures, and conventions to be employed by peers implementing the Generic Security Service Application Program Interface (as specified in RFCs 1508 [11] and 1509 [12]) when using the Simple Public-Key Mechanism." [10] The SPKM-1 GSS-API mechanism is capable of implementing both authentication exchanges described in this standard, while taking advantage of optional token fields and authentication steps in Section 3. SPKM-1 also provides implementors with a means to establish a key between the authenticating entities and protect the confidentiality of data. The SPKM-2 mechanism in [10] is not addressed in this appendix because it relies on timestamps - not signed random number challenges - to authenticate entities to one another.

By using GSS-API, entities implementing SPKM authentication can perform context establishment, algorithm negotiation and key establishment. For purposes of this appendix, non-FIPS approved security methods referenced in [10] will not be discussed in the following sections.

#### B.1 ASN.1 Specification of SPKM Tokens and Messages

SPKM describes the various GSS-API tokens that are to be passed between entities to perform unilateral and mutual authentication. This section describes the formats of those tokens in ASN.1 notation, which is explained in Appendix A, Section A.1. What follows is not a complete list of ASN.1 formatted tokens for the SPKM-1 mechanism, and this list does not completely describe those tokens or the steps necessary for performing SPKM-1 authentication using GSS-API. For example, other optional SPKM GSS-API tokens (not equivalent to authentication tokens described in this FIPS) may be implemented to provide for the data integrity and encryption of the SPKM-1 authentication tokens (SPKM-REQ, SPKM-REP-TT, and SPKM-REP-IT). Such GSS-API tokens may also be used for error recovery during an authentication exchange. The implementor should consult the SPKM specification in [10] to obtain complete details on implementing an SPKM-1 mechanism.

In the token and message descriptions below, SPKM terminology differs slightly from terminology defined in Section 2.3 of this FIPS. The SPKM specification refers to an "initiator" and "target". When performing either unilateral or mutual SPKM-1 authentication, the "initiator"



is the equivalent of entity B in this FIPS, and the "target" is the equivalent of entity A. The "initiator" in SPKM authentication is actually the "responder" described in the mutual authentication exchange in Section 3.3.

```

SpkmGssTokens      {iso(1) identified-organization(3) dod(6) internet(1)
                    security(5) mechanisms(5) spkm(1) spkmGssTokens(10)}

-- types --

CertificationData ::= SEQUENCE {
    certificationPath      [0]    CertificationPath OPTIONAL,
    certificateRevocationList [1]  CertificateList OPTIONAL
} -- at least one of the above shall be present

CertificationPath ::= SEQUENCE {
    userId      [0]    OCTET STRING OPTIONAL,
    userCertif  [1]    Certificate OPTIONAL,
    verifyKeyId [2]    OCTET STRING OPTIONAL,
    userVerifCertif [3] Certificate OPTIONAL,
    theCACertificates [4] SEQUENCE OF CertificatePair OPTIONAL
} -- Presence of [2] or [3] implies that [0] or [1] must also be
-- present. Presence of [4] implies that at least one of [0], [1],
-- [2], and [3] must also be present.

-- The requestToken in SPKM-REQ represents TokenBA, in the FIPS --
-- authentication exchanges. It contains B's random challenge to A. --

SPKM-REQ ::= SEQUENCE {
    requestToken      REQ-TOKEN,
    certif-data      [0]    CertificationData OPTIONAL,
    auth-data        [1]    AuthorizationData OPTIONAL
}

REQ-TOKEN ::= SEQUENCE {
    req-contents      Req-contents,
    algId             AlgorithmIdentifier,
    req-integrity      Integrity -- "token" is Req-contents
}

Integrity ::= BIT STRING
-- See the special note in [10] regarding this type.

Req-contents ::= SEQUENCE {
    tok-id             INTEGER (256), -- shall contain 0100 (hex)
    context-id         Random-Integer,
    pvno              BIT STRING,
    timestamp          UTCTime OPTIONAL,
    randSrc            Random-Integer,
    targ-name          Name,
    src-name           [0]    Name OPTIONAL,
    req-data            Context-Data,
    validity           [1]    Validity OPTIONAL,
    key-estb-set        Key-Estb-Algs,
    key-estb-req        BIT STRING OPTIONAL,
    key-src-bind        OCTET STRING OPTIONAL
}

Random-Integer ::= BIT STRING

```

```

Context-Data ::= SEQUENCE {
    channelId
    seq-number
    options
    conf-alg
    intg-alg
    owf-alg
}

ChannelId ::= OCTET STRING

Options ::= BIT STRING {
    delegation-state (0),
    mutual-state (1),
    replay-det-state (2),
    sequence-state (3),
    conf-avail (4),
    integ-avail (5),
    target-certif-data-required (6)
}

Conf-Algs ::= CHOICE {
    algs          [0]      SEQUENCE OF AlgorithmIdentifier,
    null          [1]      NULL
} -- confidentiality algorithms

Intg-Algs ::= SEQUENCE OF AlgorithmIdentifier -- integrity algorithms

OWF-Algs ::= SEQUENCE OF AlgorithmIdentifier

Key-Estb-Algs ::= SEQUENCE OF AlgorithmIdentifier -- key establishment
-- algorithms

AlgorithmIdentifier ::= SEQUENCE {
    algorithm      OBJECT IDENTIFIER,
    parameter      ANY DEFINED BY algorithm OPTIONAL
} -- Note that the 1993 AuthenticationFramework module in [6] uses
-- different syntax for this construct.

-- The responseToken in SPKM-REP-TI represents TokenAB in the FIPS --
-- authentication exchanges. It contains A's signature on B's challenge, --
-- and a random challenge to B during mutual authentication. --

SPKM-REP-TI ::= SEQUENCE {
    responseToken      REP-TI-TOKEN,
    certif-data        CertificationData OPTIONAL
    -- present if target-certif-data-required option was
    -- set to TRUE in SPKM-REQ
}

REP-TI-TOKEN ::= SEQUENCE {
    rep-ti-contents    Rep-ti-contents,
    algid              AlgorithmIdentifier,
    rep-ti-integ       Integrity -- "token" is Rep-ti-contents
}

```

```

Rep-ti-contents ::= SEQUENCE {
    tok-id                INTEGER (512), -- shall contain 0200 (hex)
    context-id            Random-Integer,
    pvno                  BIT STRING OPTIONAL,
    timestamp              UTCTime OPTIONAL,
    randTarg              Random-Integer,
    src-name              Name OPTIONAL,
    targ-name             Name OPTIONAL,
    randSrc               Random-Integer,
    rep-data              Context-Data,
    validity              Validity OPTIONAL,
    key-estb-id           AlgorithmIdentifier OPTIONAL,
    key-estb-str          BIT STRING OPTIONAL
}

-- The responseToken in SPKM-REP-IT represents TokenBA, in the FIPS --
-- mutual authentication exchange. It contains B's signature on --
-- A's random challenge. --

SPKM-REP-IT ::= SEQUENCE {
    responseToken          REP-IT-TOKEN,
    algid                 AlgorithmIdentifier,
    rep-it-integ           Integrity -- "token" is REP-IT-TOKEN
}

REP-IT-TOKEN ::= SEQUENCE {
    tok-id                INTEGER (768), -- shall contain 0300 (hex)
    context-id            Random-Integer,
    randSrc               Random-Integer,
    randTarg              Random-Integer,
    targ-name             Name,
    src-name              Name OPTIONAL,
    key-estb-rep          BIT STRING OPTIONAL
}

-- other types --

-- from [11] --

MechType ::= OBJECT IDENTIFIER

InitialContextToken ::= [APPLICATION 0] IMPLICIT SEQUENCE {
    thisMech              MechType,
    innerContextToken     SPKMInnerContextToken
    -- when thisMech is SPKM-1 or SPKM-2
}

SPKMInnerContextToken ::= CHOICE {
    req                   [0] SPKM-REQ,
    rep-ti                [1] SPKM-REP-TI,
    rep-it                [2] SPKM-REP-IT,
    error                 [3] SPKM-ERROR,
    mic                   [4] SPKM-MIC,
    wrap                  [5] SPKM-WRAP,
    del                   [6] SPKM-DEL
}

```

```

-- object identifier assignments --

spkm-1 OBJECT IDENTIFIER ::=
    {iso(1) identified-organization(3) dod(6) internet(1) security(5)
      mechanisms(5) spkm(1) spkm-1(1)}

-- The following two object identifiers for signature algorithms are derived
-- from "Stable Implementation Agreements for Open Systems Interconnection
-- Protocols: Part 12 - OS Security" [13]. This document was prepared by
-- the Security Special Interest Group (SECSIG) of the Open Systems
-- Environment Implementors' Workshop (OIW) hosted by NIST. The OIW has
-- registered the following algorithms with ISO. The DSA and SHA-1 are
-- examples of a current FIPS approved digital signature and secure hash
-- algorithm, respectively. Although these examples are not given in [10],
-- the SPKM specification states that the examples included in [10], "(and
-- any other algorithms) may optionally be supported by a given SPKM
-- implementation" [10].

dsaWithSHA1 OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) oiw(14) secsig(3)
    algorithm(2) 27
}

dsaCommonWithSHA1 OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) oiw(14) secsig(3)
    algorithm(2) 28      -- uses common parameters p, q, and g, which
                        -- are distributed externally
}

```

## B.2 ASN.1 Specification of Public-Key Certification Information

The SPKM-1 mechanism uses many certificate-related ASN.1 types that are derived from [6] and [9], which are either the same as or similar to the definitions listed in Section A.3 of Appendix A in this FIPS. Rather than repeat them here and note the differences, the implementor should consult Appendix B of the SPKM specification [10] for more complete details.

## Appendix C

### Example Authentication Token Formatting Based on ANSI X9.26-1990

This appendix is provided for informational purposes only, and is not part of this standard. The purpose of this appendix is to provide implementors of this standard with an optional method for formatting authentication tokens from Section 3 of this FIPS. Formatting specifications are based on message formats defined in ANSI X9.26-1990, *Financial Institution Sign-On Authentication for Wholesale Financial Transactions* [14]. Note that these formatted tokens may additionally have to be encoded before transmission, depending on the nature of a particular implementation. One possible encoding process is described in Appendix D of this standard.

#### C.1 Background

When authentication is conducted within a security services protocol, the protocol definition generally specifies where the authentication information is located and how it is represented. The individual token fields may be represented as elements in a data structure, or they may be encoded into a transmission unit using, for example, the ASN.1/DER formatting and encoding described in Appendix A. However, many implementations of the FIPS authentication protocols may not be capable of handling (or require the overhead of) ASN.1/DER formatting and encoding. Therefore, this appendix provides an ASCII-based alternative. In this appendix, the token fields are formatted based on notation and message formats in ANSI X9.26 [14]. That standard addresses several types of sign-on authentication that use secret-key, not public-key cryptography. However, with slight modifications to field tags, function definitions, and message formats, an ANSI X9.26-"like" implementation can perform either of the FIPS authentication protocols.

#### C.2 Token and Message Formats Based on ANSI X9.26

As indicated above, this appendix will allow an implementor to generate authentication tokens based on message formats described in ANSI X9.26. The abbreviations, notation, and basic functions described below were drawn from [14], with additions or slight modifications, which are marked with an asterisk ("\*").

##### C.2.1 Abbreviations

The message formats described in Table I below assume the use of certain abbreviations, some of which are based on abbreviations in [14].

Table 1: Formatting abbreviations based on ANSI X9.26

ABBREV	MEANING	REMARKS
*GRA	Entity A's Public Key Certificate	A's public key certificate binding entity A to its public/private key pair
*GRB	Entity B's Public Key Certificate	A's public key certificate binding entity B to its public/private key pair
GSM	Cryptographic Service Message	A message involved in creating a service (such as authentication) using cryptography
DATA	Data	The input of the Crypto Function (e.g., the result of the Combine Function)
*GSA	GSP generated by entity A	Output of the GSP generated with entity A's KPR
*GSB	GSP generated by entity B	Output of the GSP generated with entity B's KPR
GSP	General Security Function	* Function used to authenticate ORG to RCV
INPUT	Input	The input of the Select Function (e.g., the result of the Crypto Function)
*KPR	Private Key	Key used to generate a digital signature
MCL	Message Class	The tag for the field that defines the type of GSM
ORG	Originator	The entity sending the GSM
RCV	Recipient	The entity receiving the GSM
*SMA	Entity A's SOM	Sign-on Message with entity A's digital signature
*SMB	Entity B's SOM	Sign-on Message with entity B's digital signature
SOM	Sign-on Message	An MCL used in the sign-on authentication GSM
TTM	TVP Transmission Message	An MCL used in the sign-on authentication GSM
*TVA	Initiator's TVP	A TVP generated by the initiator, A
*TVB	Responder's TVP	A TVP generated by the responder, B
TVP	Time Variant Parameter	A random or pseudorandom number generated with a FIPS approved random number generator

## C.2.2 Notation

The following notation shall be used when formatting authentication tokens as described in Section C.2.3 of this appendix:

- 1) The character set for Cryptographic Service Messages shall be the following characters: digits (0-9), letters (A-Z), comma (,), period (.), space (**b**), solidus (/), hyphen (-), asterisk (\*), and open and close parentheses ( ( & ) ). The character (**b**) shall only be used in a message to separate fields. The character (.) shall only be used in a field to separate subfields (if required).
- 2) The presence of a Cryptographic Service Message is denoted by the field tag, "CSM".
- 3) The contents of each message shall begin with an open parenthesis "(" and end with a close parenthesis ")".
- 4) Field tags shall be separated from field contents by a solidus "/".
- 5) Fields shall be separated by a space (**b**).
- \*6) For illustration, plaintext fields are represented by "ppp"; fields containing output of the GSF are represented by "fff".
- 7) It is the responsibility of the implementor to ensure that no delimiters (e.g., "**b**" and ".") appear in the user defined fields (e.g., ORG, RCV).
- \*8) ORG and RCV refer to the two principals involved in the authentication exchange. For each token, ORG and RCV are the sender and recipient, respectively, of a CSM.
- \*9) For field tags indicating a certificate (e.g., CRA, CRB), if no certificate is present, the field contents shall consist only of a space, (**b**).

## C.2.3 Basic Functions

- \*1) The Combine Function:

The Combine Function combines multiple input values. For purposes of this appendix, the Combine Function is defined to equal the concatenation of the input values, in the order that they are listed within this function. A solidus '/' shall be used to separate the concatenated fields. In Section C.2.4 below, the Combine Function is of the following form:

Combine ( RCV,ORG,TVB,TVA )

For example, if RCV=alice, ORG=bob, TVB=abcdef01, TVA=23456789, then the result of the combine function would equal:

alice/bob/abcdef01/23456789

\*2) The Crypto Function:

The Crypto Function cryptographically transforms the input DATA (e.g., the result of the Combine Function), using the CSM sender's (ORG) private key, KPRI. For purposes of this appendix, the Crypto Function shall use a FIPS approved digital signature algorithm (e.g., the Digital Signature Algorithm specified in FIPS PUB 186) to generate a digital signature. In Section C.2.4 below, the Crypto Function is of the following form:

Crypto( KPRI, DATA )

where DATA equals the result of the Combine Function in (1) above.

\*3) The Select Function:

The Select Function selects and returns all or part of the data from INPUT (e.g., the result of the Crypto Function), facilitating the compression of messages. For purposes of this appendix, the Select Function will select all *n* bits of INPUT. In Section C.2.4 below, the Select Function is of the following form:

Select ( INPUT )

where INPUT equals the result of the Crypto Function in (2) above

\*4) The General Security Function (GSF), is used to authenticate one entity to another. In Section C.2.4 below, the GSF is formed by composing the previously described functions as follows:

GSF( PRI, RCV, ORG, TVB, TVA ) =

Select( Crypto( KPRI, Combine( RCV, ORG, TVB, TVA ) ) )

#### C.2.4 Message Formats

In each of the messages described below, the message class tag (MCL) and the field value which follows are considered to be a TokenID. In MessageAB and MessageBA2, each included certificate should have a predefined format, which is left to the implementor to define. The message formats for entity authentication tokens, based on modified ANSI X9.26 specifications, are as follows:



**TokenBA<sub>1</sub>:** In both the unilateral and mutual exchanges, the first message is a random challenge sent from B to A. The message (MessageBA1) that includes TokenBA<sub>1</sub> ("RCV/...TVB/ppp") is:

MessageBA1 =  
CSM (MCL/TTM<sub>B</sub>RCV/ppp<sub>B</sub>ORG/ppp<sub>B</sub>TVB/ppp<sub>B</sub>)

TTM TVP Transmission Message indicator (message class)  
RCV Identity of message recipient, entity A  
ORG Identity of message sender, entity B  
TVB Random number, in hexadecimal format, generated by entity B, the message sender

---

**TokenAB:** In both the unilateral and mutual exchanges, the second token is a response to B's random challenge. Also included in the token is a random number generated by A. The message (MessageAB) that includes TokenAB ("RCV/...GSA/fff") is:

MessageAB =  
CSM (MCL/SMA<sub>B</sub>RCV/ppp<sub>B</sub>ORG/ppp<sub>B</sub>TVB/ppp<sub>B</sub>TVA/ppp<sub>B</sub>GSA/fff<sub>B</sub>CRA/ppp<sub>B</sub>)

SMA Entity A's Sign-on Message indicator (message class)  
RCV Identity of message recipient, entity B  
ORG Identity of message sender, entity A  
TVB Random number, in hexadecimal format, generated by entity B, the message recipient  
TVA Random number, in hexadecimal format, generated by entity A, the message sender  
GSA The output of the GSF generated by entity A.  
CRA Entity A's public key certificate (optional).

---

**TokenBA<sub>2</sub>:** In the mutual authentication exchange, a third message is sent, which includes B's response to A's random challenge. The message (MessageBA2) that includes TokenBA<sub>2</sub> ("RCV/...GSB/fff") is:

MessageBA2 =  
CSM (MCL/SMB<sub>B</sub>RCV/ppp<sub>B</sub>ORG/ppp<sub>B</sub>TVB/ppp<sub>B</sub>TVA/ppp<sub>B</sub>GSB/fff<sub>B</sub>CRB/ppp<sub>B</sub>)

SMB Entity B's Sign-on Message indicator (message class)  
RCV Identity of message recipient, entity A  
ORG Identity of message sender, entity B

- TVB Random number, in hexadecimal format, generated by entity B, the message sender
- TVA Random number, in hexadecimal format, generated by entity A, the message recipient
- GSB The output of the GSF generated by entity B.
- CRB Entity B's public key certificate (optional).
-

## Appendix D

### Example Entity Authentication Exchange Using Base64 Encoding

This appendix is provided for informational purposes only, and is not part of this standard. The purpose of this appendix is to provide implementors of this standard with an optional method for encoding authentication tokens. The method described below for encoding formatted tokens is Base64 Content-Transfer-Encoding, defined in Internet RFC 1521, MIME (Multipurpose Internet Mail Extensions) Part One [15]. By converting data to ASCII characters, this encoding method allows authentication tokens to be exchanged over unstructured, non-binary channels. Note that this encoding method is independent of the format of the authentication tokens. For example, ASN.1/DER-encoded tokens from Appendices A and B might also be base64-encoded, depending on the transmission channel's ability to handle binary data. Also, there exist other, similar encoding schemes that may provide more suitable alternatives for a particular implementation. Section D.5 will present an example of using base64 encoding with authentication tokens described in Appendix C, even though they are already formatted using only ASCII characters.

#### D.1 Background

When authentication is conducted within a security services protocol, the protocol definition generally specifies where the authentication information is located and how it is represented. Once the authentication information is formatted, it may then have to be encoded in a binary form. If the channel being used to transmit the authentication information is incapable of handling binary data, one possible solution is to further encode the data using base64 encoding as defined in [15].

Regardless of the encoding method used (prior to performing base64 encoding), a formatted authentication message will be referred to in this appendix as a "transfer string", which is simply a sequence of octets with known length. The method for encoding the transfer string is independent of the method used to format the transfer string; however, this appendix describes the use of Base64 Content-Transfer-Encoding [15].

Protocols which explicitly support security services are able to carry authentication transfer strings as-is. However, channels which have no protocol support for security services may also require strong authentication. In such cases the authentication information is carried "in-band" as part of the normal user data. This presents two potential problems: the authentication data does not necessarily appear at a fixed location, and the channel may not be able to pass arbitrary binary information. The format specified in this appendix addresses both problems.

- Tokens begin with a fixed label (token identifier); receivers can scan an incoming data stream for labels to locate potential authentication tokens.
- The token data is converted to a text representation designed to pass through most channels without difficulty.

## D.2 Base64 Content-Transfer-Encoding

Assuming that a transfer string has been generated for an authentication token, the encoding of that token must take place before including it in an "in-band" transmission. The transfer string may be converted to a base64 string according to the procedure defined in Internet RFC 1521. The following description is adapted from [15], Section 5.2:

The Base64 Content-Transfer-Encoding is designed to represent arbitrary sequences of octets in a form that need not be humanly readable. The encoding and decoding algorithms are simple, but the encoded data are consistently only about 33 percent larger than the unencoded data. . . . A 65-character subset of US-ASCII is used, enabling 6 bits to be represented per printable character. (The extra 65th character, "=", is used to signify a special processing function). . . .

The encoding process represents 24-bit groups of input bits as output strings of [four] encoded characters. Proceeding from left to right, a 24-bit input group is formed by concatenating [three] 8-bit input groups. These 24 bits are then treated as [four] concatenated 6-bit groups, each of which is translated into a single digit in the base64 alphabet. When encoding a bit stream via the base64 encoding, the bit stream must be presumed to be ordered with the most-significant-bit first. That is, the first bit in the stream will be the high-order bit in the first byte, and the eighth bit will be the low-order bit in the first byte, and so on.

Table II: The Base64 Alphabet

Value	Encoding	Value	Encoding	Value	Encoding	Value	Encoding
0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1
3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	p	58	6
8	I	25	Z	42	q	59	7
9	J	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/
13	N	30	e	47	v		
14	O	31	f	48	w	(pad)	=
15	P	32	g	49	x		
16	Q	33	h	50	y		

Each 6-bit group is used as an index into an array of 64 printable characters. The character referenced by the index is placed in the output string. These characters, identified in [Table II], are selected so as to be universally representable. . . .

The output stream (encoded bytes) must be represented in lines of no more than 76 characters each. All line breaks or other characters not found in [Table II] must be ignored by decoding software. In base64 data, characters other than those in [Table II], line breaks, and other white space probably indicate a transmission error, about which a warning message or even a message rejection might be appropriate under some circumstances.

Special processing is performed if fewer than 24 bits are available at the end of the data being encoded. A full encoding [unit] is always completed at the end of a body. When fewer than 24 input bits are available in an input group, zero bits are added (on the right) to form an integral number of 6-bit groups. Padding at the end of the data is performed using the '=' character. Since all base64 input is an integral number of octets, only the following cases can arise: (1) the final [unit] of encoding input is an integral multiple of 24 bits; here, the final unit of encoded output will be an integral multiple of [four] characters with no '=' padding, (2) the final [unit] of encoding input is exactly 8 bits; here, the final unit of encoded output will be two characters followed by two '=' padding characters, or (3) the final [unit] of encoding input is exactly 16 bits; here, the final unit of encoded output will be three characters followed by one '=' padding character. [15]

### D.3 Format of In-Band Authentication Messages

Once a token's transfer string has been base64-encoded, it can then be formatted into a message of the form:

Label":"base64-string";

The label identifies the type of token being sent, and may be considered to be the TokenID (or part of the TokenID) specified in the FIPS authentication protocols. Labels have been given the "FIPSEA" prefix, which stands for "FIPS Entity Authentication":

FIPSEA_BA1	-Initial token from B to A in both Unilateral and Mutual exchanges.
FIPSEA_AB	-Response token from A to B in both Unilateral and Mutual exchanges.
FIPSEA_BA2	-Response token from B to A in the Mutual exchange.

The base64-string is delimited by colon (:) characters to allow its extent to be determined unambiguously. The initial colon must immediately follow the Label with no intervening whitespace or other characters. The base64-string may include line breaks or other whitespace, as specified in Section D.2.

#### D.4 Error detection

This formatting method does not explicitly include any error control mechanisms, although it does allow some sanity checks to be applied to received data. Because they are used only at the end of the data, the occurrence of any '=' or ':' characters may be taken as evidence that the end of the data has been reached without truncation in transit. The occurrence of any non-whitespace characters between the '=' characters (if any) and the trailing ':' indicates an error in transit. Any errors in the label/initial colon and any non-base64 character before the final colon should cause the token to be treated as corrupt.

Explicit error control coding (to enable more extensive error detection or correction) can be applied as part of the encoding method, or as a separate step after encoding but before formatting.

#### D.5 Example

For purposes of example, the authentication messages from Appendix C will be base64-encoded. In many cases, those messages will not need to be encoded, since they are likely to be in ASCII-only format. However, this example will be used to demonstrate both the ANSI X9.26-based formatting and the base64 encoding. The digital signatures in MessageAB and MessageBA2 will be generated using the Digital Signature Algorithm specified in FIPS PUB 186, and no certificates will be included. The base64 encoding is generated beginning with the characters "CSM" and ending with the close parenthesis ")" for each message.

##### Mutual entity authentication:

Entity A's ID=               alice  
Entity A's TVP=             d6f47bc433299436  
Entity A's private key (hex)= 374b8a09ae40ced4d9510256bf7f3262679e3b3f

Entity B's ID=               bob  
Entity B's TVP=             e69dfb21ffd051a3  
Entity B's private key (hex): 390382c6aa978875ec7f3160bc9d675e430da255

-----

MessageBA1 =

CSM(MCL/SMA RCV/alice ORG/bob TVB/e69dfb21ffd051a3)

Once this message is labeled and base64-encoded, the result is:

FIPSEA\_BA1:Q1NNKE1DTC9TTUEgUkNWL2FsaWNlIE9SRy9ib2IyVZVZCL2U2OWRmYjIxZmZmkMD  
UxYTMp:

-----

MessageAB =

CSM(MCL/SMA RCV/bob ORG/alice TVB/e69dfb21ffd051a3 TVA/d6f47bc433299436  
GSA/b172f97910da3e5dde070c2af334eaa349063695938969d02882a8a7736015e081a38  
cf8fd33844c CRA/ )

Once this message is labeled and base64-encoded, the result is:

FIPSEA\_AB:Q1NNKE1DTC9TTUBgUkNWL2JvYiBPukcvYwXpY2DgVfZCL2U2OWRmYjIxZmZkMDU  
xYTMgVfZBL2Q2ZjQ3YmM0MzMzMyOTk0MzYgR1NBL2IXNzJmOTc5MTBkYTN1NWRkZTA3MGMyYwYz  
MzR1YWEzNDkwNjM2OTU5Mzg5NjlkMDI4ODJhOGU3NzH2MD81ZTA4MWEzOGNmOGZkMzM4NDRjI  
ENSQS8gKQ==:

-----

MessageBA2 =

CSM(MCL/SMB RCV/alice ORG/bob TVB/e69dfb21ffd051a3 TVA/d6f47bc433299436  
GSB/c26ac822a93d5c349962d1a78a229d27abfea415b934b2604e6facce2c233afc59be6  
be6a9e262f5 CRB/ )

Once this message is labeled and base64-encoded, the result is:

FIPSEA\_BA2:Q1NNKE1DTC9TTUIGuKNWL2FsaWN1IE9SRy91b2IgvfZCL2U2OWRmYjIxZmZkMDU  
UxYTMgVfZBL2Q2ZjQ3YmM0MzMzMyOTk0MzYgR1NCL2MyNmFjODIyYTkzZDVjMzQ5OTYyZDFhNzh  
hMjI5ZDI3YWJmZW80MTViOTM0YjI2MDRlNmZhY2NlMmMyMzNhZmMlOWJlNmJlNmE5ZTI2MmY1  
IENSQ18gKQ==:

-----

## Appendix E

### Selected References

- [1] ISO/IEC JTC 1/SC 21 N9148, Final Draft, ITU-T Rec. X.680 | ISO/IEC 8824-1, Information Technology - Abstract Syntax Notation One (ASN.1) - Specification of Basic Notation, November 15, 1994.
- [2] ISO/IEC JTC 1/SC 21 N9149, Final Draft, ITU-T Rec. X.681 | ISO/IEC 8824-2, Information Technology - Abstract Syntax Notation One (ASN.1) - Information Object Specification, November 15, 1994.
- [3] ISO/IEC JTC 1/SC 21 N9151, Final Draft, ITU-T Rec. X.682 | ISO/IEC 8824-3, Information Technology - Abstract Syntax Notation One (ASN.1) - Constraint Specification, November 15, 1994.
- [4] ISO/IEC JTC 1/SC 21 N9152, Final Draft, ITU-T Rec. X.683 | ISO/IEC 8824-4, Information Technology - Abstract Syntax Notation One (ASN.1) - Parameterization of ASN.1 Specifications, November 15, 1994.
- [5] ISO/IEC JTC 1/SC 21 N9153, Final Draft, ITU-T Rec. X.690 | ISO/IEC 8825-1, Information Technology - Abstract Syntax Notation One (ASN.1) - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), November 15, 1994.
- [6] ITU-T Rec. X.509 | ISO/IEC 9594-8, Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Editor's DRAFT, February 14, 1993.
- [7] Draft Amendments DAM 4 to ISO/IEC 9594-2, DAM 2 to ISO/IEC 95-94-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC 9594-8 on Certificate Extensions, Editor's DRAFT, August 1, 1995.
- [8] ITU-T X.520 | ISO 9594-6, Information technology - Open Systems Interconnection - The Directory: Selected Attribute Types, Editor's DRAFT, February 14, 1993.
- [9] ITU-T Rec. X.501 | ISO/IEC 9594-2, Information Technology - Open Systems Interconnection - The Directory: The Models, Editor's DRAFT, February 14, 1993.
- [10] Adams, C., The Simple Public-Key GSS-API Mechanism (SPKM), Internet Proposed Standard RFC 2025, October 1996.
- [11] Linn, J., Internet RFC 1508 - Generic Security Service Application Program Interface, September 1993.



- [12] Wray, J., Internet RFC 1509 - Generic Security Service API: C-bindings, September 1993.
  - [13] Mirhakkak, Dr. Mohammad, ed., Stable Implementation Agreements for Open Systems Interconnection Protocols: Part 12 - OS Security, June 1995.
  - [14] ANSI X9.26, Financial Institution Sign-On Authentication for Wholesale Financial Transactions, Approved February 28, 1990.
  - [15] Borenstein, N. and N. Freed, Internet RFC 1521 - MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies, September 1993.
-



## **Exhibit B**



**National Standard of Canada**  
**CAN/CSA-ISO/IEC 9798-3:02**  
**(ISO/IEC 9798-3:1998)**

International Standard **ISO/IEC 9798-3:1998 (second edition, 1998-10-15)** has been adopted without modification (IDT) as CSA Standard **CAN/CSA-ISO/IEC 9798-3:02**, which has been approved as a National Standard of Canada by the Standards Council of Canada.  
*ISBN 1-55324-966-6*

*December 2002*

---

**Information technology — Security  
techniques — Entity authentication —**

**Part 3:**  
**Mechanisms using digital signature techniques**

*Technologies de l'information — Techniques de sécurité — Authentification  
d'entité —*

*Partie 3: Mécanismes utilisant des techniques de signature numériques*



Reference number  
ISO/IEC 9798-3:1998(E)

**The Canadian Standards Association (CSA),** under whose auspices this National Standard has been produced, was chartered in 1919 and accredited by the Standards Council of Canada to the National Standards system in 1973. It is a not-for-profit, nonstatutory, voluntary membership association engaged in standards development and certification activities.

CSA standards reflect a national consensus of producers and users — including manufacturers, consumers, retailers, unions and professional organizations, and governmental agencies. The standards are used widely by industry and commerce and often adopted by municipal, provincial, and federal governments in their regulations, particularly in the fields of health, safety, building and construction, and the environment.

Individuals, companies, and associations across Canada indicate their support for CSA's standards development by volunteering their time and skills to CSA Committee work and supporting the Association's objectives through sustaining memberships. The more than 7000 committee volunteers and the 2000 sustaining memberships together form CSA's total membership from which its Directors are chosen. Sustaining memberships represent a major source of income for CSA's standards development activities.

The Association offers certification and testing services in support of and as an extension to its standards development activities. To ensure the integrity of its certification process, the Association regularly and continually audits and inspects products that bear the CSA Mark.

In addition to its head office and laboratory complex in Toronto, CSA has regional branch offices in major centres across Canada and inspection and testing agencies in eight countries. Since 1919, the Association has developed the necessary expertise to meet its corporate mission: CSA is an independent service organization whose mission is to provide an open and effective forum for activities facilitating the exchange of goods and services through the use of standards, certification and related services to meet national and international needs.

For further information on CSA services, write to Canadian Standards Association  
5060 Spectrum Way, Suite 100  
Mississauga, Ontario, L4W 5N6  
Canada



**The Standards Council of Canada** is the coordinating body of the National Standards system, a federation of independent, autonomous organizations working towards the further development and improvement of voluntary standardization in the national interest.

The principal objects of the Council are to foster and promote voluntary standardization as a means of advancing the national economy, benefiting the health, safety, and welfare of the public, assisting and protecting the consumer, facilitating domestic and international trade, and furthering international cooperation in the field of standards.

A National Standard of Canada is a standard which has been approved by the Standards Council of Canada and one which reflects a reasonable agreement among the views of a number of capable individuals whose collective interests provide to the greatest practicable extent a balance of representation of producers, users, consumers, and others with relevant interests, as may be appropriate to the subject in hand. It normally is a standard which is capable of making a significant and timely contribution to the national interest.

Approval of a standard as a National Standard of Canada indicates that a standard conforms to the criteria and procedures established by the Standards Council of Canada. Approval does not refer to the technical content of the standard; this remains the continuing responsibility of the accredited standards-development organization.

Those who have a need to apply standards are encouraged to use National Standards of Canada whenever practicable. These standards are subject to periodic review; therefore, users are cautioned to obtain the latest edition from the organization preparing the standard.

The responsibility for approving National Standards of Canada rests with the Standards Council of Canada  
270 Albert Street, Suite 200  
Ottawa, Ontario, K1P 6N7  
Canada



*Although the intended primary application of this Standard is stated in its Scope, it is important to note that it remains the responsibility of the users to judge its suitability for their particular purpose.*

<sup>®</sup>Registered trade-mark of Canadian Standards Association

# CAN/CSA-ISO/IEC 9798-3:02

## **Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques**

### **CSA Preface**

Standards development within the Information Technology sector is harmonized with international standards development. Through the CSA Technical Committee on Information Technology (TCIT), Canadians serve as the Canadian Advisory Committee (CAC) on ISO/IEC Joint Technical Committee 1 on Information Technology (ISO/IEC JTC1) for the Standards Council of Canada (SCC), the ISO member body for Canada and sponsor of the Canadian National Committee of the IEC. Also, as a member of the International Telecommunication Union (ITU), Canada participates in the International Telegraph and Telephone Consultative Committee (ITU-T).

This Standard supersedes CAN/CSA-ISO/IEC 9798-3-94 (adoption of ISO/IEC 9798-3:1993).

This International Standard was reviewed by the CSA TCIT under the jurisdiction of the Strategic Steering Committee on Information Technology and deemed acceptable for use in Canada. (A committee membership list is available on request from the CSA Project Manager.) From time to time, ISO/IEC may publish addenda, corrigenda, etc. The CSA TCIT will review these documents for approval and publication. For a listing, refer to the CSA Information Products catalogue or *CSA Info Update* or contact a CSA Sales representative. This Standard has been formally approved, without modification, by the Technical Committee and has been approved as a National Standard of Canada by the Standards Council of Canada.

December 2002

© Canadian Standards Association — 2002

All rights reserved. No part of this publication may be reproduced in any form whatsoever without the prior permission of the publisher. ISO/IEC material is reprinted with permission. Where the words “this International Standard” appear in the text, they should be interpreted as “this National Standard of Canada”.

Inquiries regarding this National Standard of Canada should be addressed to  
Canadian Standards Association  
5060 Spectrum Way, Suite 100, Mississauga, Ontario, Canada L4W 5N6  
1-800-463-6727 • 416-747-4044  
[www.csa.ca](http://www.csa.ca)

---

**Information technology — Security  
techniques — Entity authentication —**

**Part 3:  
Mechanisms using digital signature techniques**

*Technologies de l'information — Techniques de sécurité — Authentification  
d'entité —*

*Partie 3: Mécanismes utilisant des techniques de signature numériques*



## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

International Standard ISO/IEC 9798-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9798-3:1993), which has been technically revised. Note, however, that implementations which comply with ISO/IEC 9798-3 (1st edition) will be compliant with ISO/IEC 9798-3 (2nd edition).

ISO/IEC 9798 consists of the following parts, under the general title *Information technology — Security techniques — Entity authentication*:

- Part 1: General
- Part 2: Mechanisms using symmetric encipherment algorithms
- Part 3: Mechanisms using digital signature techniques
- Part 4: Mechanisms using a cryptographic check function
- Part 5: Mechanisms using zero knowledge techniques

Further parts may follow.

Annex A of this part of ISO/IEC 9798 is for information only.

© ISO/IEC 1998

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland  
Printed in Switzerland

# Information technology — Security techniques — Entity authentication —

## Part 3:

### Mechanisms using digital signature techniques

#### 1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using digital signatures based on asymmetric techniques. Two mechanisms are concerned with the authentication of a single entity (unilateral authentication), while the remaining are mechanisms for mutual authentication of two entities. A digital signature is used to verify the identity of an entity. A trusted third party may be involved.

The mechanisms specified in this part of ISO/IEC 9798 use time variant parameters such as time stamps, sequence numbers, or random numbers, to prevent valid authentication information from being accepted at a later time.

If a time stamp or a sequence number is used, one pass is needed for unilateral authentication, while two passes are needed to achieve mutual authentication. If a challenge and response method employing random numbers is used, two passes are needed for unilateral authentication, while three or four passes (depending on the mechanism employed) are required to achieve mutual authentication.

#### 2 Normative reference

The following standard contains provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. At the time of publication, the edition indicated was valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 9798 are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 9798-1: 1997, *Information technology — Security techniques — Entity authentication — Part 1: General*.

#### 3 Definitions and notation

For the purposes of this part of ISO/IEC 9798 the definitions and notation described in ISO/IEC 9798-1 apply.

#### 4 Requirements

In the authentication mechanisms specified in this part of ISO/IEC 9798 an entity to be authenticated corroborates its identity by demonstrating its knowledge of its private signature key. This is achieved by the entity using its private signature key to sign specific data. The signature can be verified by anyone using the entity's public verification key.

The authentication mechanisms have the following requirements:

- a) A verifier shall possess the valid public key of the claimant, i.e., of the entity that the claimant claims to be.
- b) A claimant shall have a private signature key known and used only by the claimant.

If either of these is not satisfied then the authentication process may be compromised or it cannot be completed successfully.

#### NOTES

1 One way of obtaining a valid public key is by means of a certificate (see Annex C of ISO/IEC 9798-1). The generation, distribution, and revocation of certificates are outside the scope of this part of ISO/IEC 9798. There may exist a trusted third party for this purpose. Another way of obtaining a valid public key is by trusted courier.

2 References to digital signature schemes are contained in Annex D of ISO/IEC 9798-1.



## 5 Mechanisms

The specified entity authentication mechanisms make use of time variant parameters such as time stamps, sequence numbers or random numbers (see Annex B of ISO/IEC 9798-1 and Note 1 below).

Throughout this part of ISO/IEC 9798, tokens have the following form:

$$\text{Token} = X_1 \| \dots \| X_i \| s_{S_A}(V_1 \| \dots \| V_j).$$

In this part of ISO/IEC 9798, the term "signed data" refers to " $V_1 \| \dots \| V_j$ " used as input to the signature scheme and the term "unsigned data" refers to " $X_1 \| \dots \| X_i$ ".

If information contained in the signed data of the token can be recovered from the signature, then it need not be contained in the unsigned data of the token (see, for example, ISO/IEC 9796).

If information contained in the text field of the signed data of the token cannot be recovered from the signature, then it shall be contained in the unsigned text field of the token.

If information in the signed data of the token (e.g., a random number) is already known to the verifier, then it need not be contained in the unsigned data of the token sent by the claimant.

All text fields specified in the following mechanisms are available for use in applications outside the scope of this part of ISO/IEC 9798 (they may be empty). Their relationship and contents depend upon the specific application. See Annex A for information on the use of text fields.

### NOTES

- 1 The signing by one entity of a data block which has been manipulated by a second entity for some ulterior motive can be prevented by the first entity including its own random number in the data block which it signs. In this case, it is the unpredictability which prevents the signing of pre-defined data.
- 2 As the distribution of certificates is outside the scope of this part of ISO/IEC 9798, the sending of certificates is optional in all mechanisms.

### 5.1 Unilateral authentication

Unilateral authentication means that only one of the two entities is authenticated by use of the mechanism.

#### 5.1.1 One pass authentication

In this authentication mechanism the claimant *A* initiates the process and is authenticated by the verifier

*B*. Uniqueness / timeliness is controlled by generating and checking a time stamp or a sequence number (see Annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 1.



Figure 1

The form of the token (TokenAB), sent by the claimant *A* to the verifier *B* is:

$$\text{TokenAB} = T_{N_A} \| B \| \text{Text2} \| s_{S_A} (T_{N_A} \| B \| \text{Text1}).$$

where the claimant *A* uses either a sequence number  $N_A$  or a time stamp  $T_A$  as the time variant parameter. The choice depends on the technical capabilities of the claimant and the verifier as well as on the environment.

### NOTES

- 1 The inclusion of the identifier *B* in the signed data of TokenAB is necessary to prevent the token from being accepted by anyone other than the intended verifier.
  - 2 In general, Text2 is not authenticated by this process.
  - 3 One application of this mechanism could be key distribution (see Annex A of ISO/IEC 9798-1).
- (1) *A* sends TokenAB and, optionally, its certificate to *B*.
  - (2) On receipt of the message containing TokenAB, *B* performs the following steps:
    - (i) It ensures that it is in possession of a valid public key of *A* either by verifying the certificate of *A* or by some other means.
    - (ii) It verifies TokenAB by verifying the signature of *A* contained in the token, by checking the time stamp or the sequence number, and by checking that the value of the identifier field (*B*) in the signed data of TokenAB is equal to entity *B*'s distinguishing identifier.

### 5.1.2 Two pass authentication

In this authentication mechanism the claimant *A* is authenticated by the verifier *B* who initiates the process. Uniqueness / timeliness is controlled by generating and checking a random number  $R_B$  (see Annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 2.

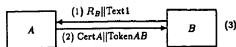


Figure 2

The form of the token (TokenAB), sent by the claimant A to the verifier B is:

$$\text{TokenAB} = R_A || R_B || B || \text{Text3} || s_A(R_A || R_B || B || \text{Text2}).$$

The inclusion of identifier B in TokenAB is optional. It depends on the environment in which this authentication mechanism is used.

#### NOTES

1 The inclusion of the optional identifier B in the signed data of TokenAB can prevent the token from being accepted by anyone other than the intended verifier (e.g., in a person-in-the-middle attack).

2 The inclusion of the random number  $R_A$  in the signed part of TokenAB prevents B from obtaining the signature of A on data chosen by B prior to the start of the authentication mechanism. This measure may be required, for example, when the same key is used by A for purposes other than entity authentication.

- (1) B sends a random number  $R_B$  and, optionally, a text field Text1 to A.
- (2) A sends TokenAB and, optionally, its certificate to B.
- (3) On receipt of the message containing TokenAB, B performs the following steps:

- (i) It ensures that it is in possession of a valid public key of A either by verifying the certificate of A or by some other means.
- (ii) It verifies TokenAB by checking the signature of A contained in the token, by checking that the random number  $R_B$ , sent to A in step (1), agrees with the random number contained in the signed data of TokenAB, and by checking that the value of the identifier field (B) in the signed data of TokenAB, if present, is equal to B's distinguishing identifier.

#### 5.2 Mutual authentication

Mutual authentication means that the two communicating entities are authenticated to each other.

The two mechanisms described in 5.1.1 and 5.1.2 are extended in 5.2.1 and 5.2.2, respectively, to achieve mutual authentication. This is done by transmitting one further message resulting in two additional steps.

The mechanism specified in 5.2.3 uses four messages which, however, need not all be sent consecutively. In this way the authentication process may be speeded up.

##### 5.2.1 Two pass authentication

In this authentication mechanism uniqueness / timeliness is controlled by generating and checking time stamps or sequence numbers (see Annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 3.

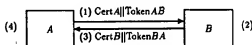


Figure 3

The form of the token (TokenAB), sent by A to B, is identical to that specified in 5.1.1.

$$\text{TokenAB} = T_A^A || B || \text{Text2} || s_A(T_A^A || B || \text{Text1}).$$

The form of the token (TokenBA), sent by B to A, is:

$$\text{TokenBA} = T_B^B || A || \text{Text4} || s_B(T_B^B || A || \text{Text3}).$$

The choice of using either time stamps or sequence numbers in this mechanism depends on the technical capabilities of the claimant and the verifier as well as on the environment.

NOTE 1 — The inclusion of identifiers A and B in the signed data of TokenBA and TokenAB, respectively, is necessary to prevent the tokens from being accepted by anyone other than the intended verifier.

Steps (1) and (2) are identical to those specified in 5.1.1, one pass authentication.

- (3) B sends TokenBA and, optionally, its certificate to A.
- (4) The message in step (3) is handled in a manner analogous to step (2) of 5.1.1.

NOTE 2 — The two messages of this mechanism are not bound together in any way, other than implicitly by timeliness; the mechanism involves independent use of mechanism 5.1.1 twice. Further binding together of these messages can be achieved by making appropriate use of the text fields.

### 5.2.2 Three pass authentication

In this authentication mechanism uniqueness / timeliness is controlled by generating and checking random numbers (see Annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 4.

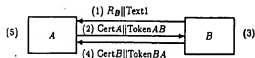


Figure 4

The tokens are of the following form:

$$\text{TokenAB} = R_A || R_B || B || \text{Text3} || S_A (R_A || R_B || B || \text{Text2}).$$
$$\text{TokenBA} = R_B || R_A || A || \text{Text5} || s_{S_B}(R_B || R_A || A || \text{Text4}).$$

The inclusion of the parameter *B* in *TokenAB* and the inclusion of the parameter *A* in *TokenBA* are optional. They depend on the environment in which this authentication mechanism is used.

NOTE — The inclusion of the random number  $R_A$  in the signed part of  $\text{TokenAB}$  prevents  $B$  from obtaining the signature of  $A$  on data chosen by  $B$  prior to the start of the authentication mechanism. This measure may be required, for example, when the same key is used by  $A$  for purposes other than entity authentication. However, the inclusion of  $R_B$  in  $\text{TokenBA}$ , whilst necessary for security reasons which dictate that  $A$  should check that it is the same as the value sent in the first message, may not offer the same protection to  $B$ , since  $R_B$  is known to  $A$  before  $R_A$  is chosen. If this type of protection is required,  $B$  can insert an additional random number  $R'_B$  in the text fields  $\text{Text4}$  and  $\text{Text5}$  of  $\text{TokenBA}$ .

- (1) *B* sends a random number  $R_B$  and, optionally, a text field *Text1* to *A*.
- (2) *A* sends *TokenAB* and, optionally, its certificate to *B*.
- (3) On receipt of the message containing *TokenAB*, *B* performs the following steps:
  - (i) It ensures that it is in possession of a valid public key of *A* either by verifying the certificate of *A* or by some other means.
  - (ii) It verifies *TokenAB* by checking the signature of *A* contained in the token, by checking that the random number  $R_B$ , sent to *A* in step (1), agrees with the random number contained in the signed data of *TokenAB*, and by checking that the value of the identifier field (*B*) in the signed data of *TokenAB*, if present, is equal to *B*'s distinguishing identifier.

- (4) *B* sends Token*BA* and, optionally, its certificate to *A*.
- (5) On receipt of the message containing Token*BA*, *A* analogously performs steps (i) and (ii) listed under (3). In addition, *A* checks that the random number *R<sub>B</sub>* contained in the signed data of Token*BA* is equal to the random number *R<sub>B</sub>* received in step (1).

### 5.2.3 Two pass parallel authentication

In this mechanism authentication is carried out in parallel. Uniqueness / timeliness is controlled by generating and checking random numbers (see Annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 5.

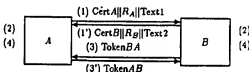


Figure 5

The tokens are similar to those of clause 5.1.2:

$$\text{Token}_{AB} = R_A || R_B || B || \text{Text}_4 || S_A (R_A || R_B || B || \text{Text}_3)$$
$$\text{Token}_{BA} = R_B \| R_A \| A \| \text{Text6} \| S_B (R_B \| R_A \| A \| \text{Text5}).$$

The inclusion of the parameter  $B$  in  $\text{Token}_{AB}$  and the inclusion of the parameter  $A$  in  $\text{Token}_{BA}$  are optional. They depend on the environment in which this authentication mechanism is used.

NOTE 1 — The random number  $R_A$  is present in TokenAB to prevent B from obtaining the signature of A on data chosen by B prior to the start of the authentication mechanism. This prevention may be required, for example, when the same key is used by A for other purposes in addition to entity authentication. For similar reasons the random number  $R_B$  is present in TokenBA. Depending on the relative time of receipt of the messages sent in steps (1) and (1'), one of the parties may know the random number of the other party when choosing its random number. If this is undesirable, both parties can insert an additional random number  $R'_A$  and  $R'_B$  in the text fields Text3 and Text4 of TokenAB, and Text5 and Text6 of TokenBA, respectively.

- (1') *B* sends  $R_B$  and, optionally, its certificate and a text field Text2 to *A*.

- (2) *A* and *B* ensure that they are in possession of a valid public key of the other entity either by verifying the respective certificate or by some other means.
- (3) *A* sends Token $AB$  to *B*.
- (3') *B* sends Token $BA$  to *A*.
- (4) *A* and *B* perform the following steps:

Each of them verifies the received token by checking the signature contained in the token and by checking that the random number, which it previously sent to the other entity, agrees with the random number contained in the signed data of the token received.

NOTE 2 — An alternative to mechanism 5.2.3 is to run mechanism 5.1.2 both ways. The inclusion of the certificates in the first messages of mechanism 5.2.3 allows for earlier certificate verification which may speed up the authentication process.

## Annex A

### (informative)

#### Use of text fields

The tokens specified in clause 5 of this part of ISO/IEC 9798 contain text fields. The actual use of and the relationships between the various text fields in a given pass depend on the application. Some examples are given below; see also Annex A of ISO/IEC 9798-1.

If a signature scheme without message recovery is used and if the signed text field is not empty, then the verifier needs to be in possession of the text prior to verifying the signature. In this Annex "signed text fields" refers to text fields in the signed data and "unsigned text fields" refers to text fields in the unsigned data.

For example, if a digital signature scheme without message recovery is used, any information requiring data origin authentication should be placed in the signed text field and (as part of) the unsigned text field in the token.

If the tokens do not contain (sufficient) redundancy, the signed text fields may be used to provide additional redundancy.

Signed text fields may be used to indicate that the token is only valid for the purpose of entity authentication. Should there be a concern that one entity might choose a "degenerate" value with malicious intent for the other entity to sign, the other entity may introduce a random number in the text field.

Should an algorithm be used where it may be possible to launch attacks based on the fact that a particular claimant is using the same key for all verifiers with which the claimant communicates, and if such attacks are considered to be a threat, the identity of the intended verifier should be included in the signed text field and, if necessary, in the unsigned text field.

Unsigned text fields can also be used to provide information to a verifier indicating the (unauthenticated) identity which a claimant is claiming. If means other than certificates are used for distributing public keys, such information may be required to allow a verifier to determine which public key is to be used to authenticate a claimant.



## Exhibit C

Response To Notice To File Missing Parts Of Application  
Filing Date Granted (PTO-1533)(Large Entity)

Docket No.  
112-0019US

In Re Application

James Kleinstein

Serial No.  
10/062,853

Filing Date  
1/31/2002

Examiner

Group Art Unit

Invention:

**NODE AND PORT AUTHENTICATION IN A FIBRE CHANNEL NETWORK**

TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Box Missing Parts

This is a response to the Notice to File Missing Parts of Application - Filing Date Granted (PTO-1533) mailed on  
2/28/2002  
Date

Enclosed herewith for filing are the following:

- ☒ A copy of the Notice to File Missing Parts of Application - Filing Date Granted (PTO-1533). (REQUIRED)
- ☒ An oath or declaration in compliance with 37 CFR 1.63, including residence information and identifying the application by the above Application Number and Filing Date.
- ☐ A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date.
- ☐ An oath or declaration in compliance with 37 CFR 1.63 listing the names of all inventors and signed by the omitted inventor(s), identifying this application by the above Application Number and Filing Date.
- ☐ A verified English translation of the non-English language application papers as originally filed. It is requested that this translation be used as the copy for examination purposes in the United States Patent and Trademark Office.
- ☒ Other (list):

Power of Attorney or Authorization of Agent;  
Statement Under 37 CFR 3.73(b);  
Petition for Acceptance of National Application without  
Participation of One or More Inventor Under 37 C.F.R. 1.47;  
Declaration of Louis Brucculeri in Support of Petition under § 1.47  
Check for \$370.00  
Assignment, PTO-1535, \$40 check

**Response To Notice To File Missing Parts Of Application**  
**Filing Date Granted (PTO-1533)(Large Entity)**

Docket No.  
112-0019US

In Re Application Of:  
**James Kleinsteinber**

Serial No.  
10/062,853

Filing Date  
1/31/2002

Examiner

Group Art Unit

Invention:

**NODE AND PORT AUTHENTICATION IN A FIBRE CHANNEL NETWORK**

TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Box Missing Parts

☒ Completion of application fees as calculated below:

☐ Utility application filing fee \_\_\_\_\_

☐ Design application filing fee \_\_\_\_\_

☐ Total number of independent claims = \_\_\_\_\_

☐ Total number of claims = \_\_\_\_\_

☐ Multiple dependent claims \_\_\_\_\_

☒ Surcharge for late payment of filing fee and/or late filing of original declaration or oath \$130.00

☒ Petition and fee for filing by other than all the inventors or a person not the inventor \$130.00

☐ Fee for processing an application filed with a non-English language specification \_\_\_\_\_

☐ Fee for processing and retention of application \_\_\_\_\_

Total completion of application fees \$260.00

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a response to the above-identified Notice to File Missing Parts of Application. The requested extension is as follows (check time period desired). If an additional time extension is required, please consider this a petition therefor.

☒ One month    ☐ Two months    ☐ Three months    ☐ Four months    ☐ Five months

from: April 28, 2002                      until: May 28, 2002  
*Date* *Date*

Total time extension fees \$110.00

Total fees due \$370.00



Response To Notice To File Missing Parts Of Application  
Filing Date Granted (PTO-1533) (Large Entity)

Docket No.  
112-0019US

In Re Application Of:

James Kleinsteinber

Serial No.  
10/062,853

Filing Date  
1/31/2002

Examiner

Group Art Unit

Invention:


**NODE AND PORT AUTHENTICATION IN A FIBRE CHANNEL NETWORK**

TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Box Missing Parts

The fee of \$370.00 is to be paid as follows:

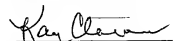
- ☒ A check in the amount of the fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. 501922  
A duplicate copy of this sheet is enclosed.
- ☐ If an additional extension of time is required, please consider this a petition therefor and charge any additional fees which may be required to Deposit Account No.  
A duplicate copy of this sheet is enclosed.

  
Signature

Dated: 5/28/02

Louis Brucculeri, Reg. No. 38,834  
Wong, Cabello, Lutsch, Rutherford & Brucculeri PC  
20333 SH 249 Suite 600  
Houston, TX 77070  
832 446-2415  
Fax 832 446-2424

I certify that this document and fee is being deposited on  
5/28/2002 with the U.S. Postal Service as first  
class mail under 37 C.F.R. 1.8 and is addressed to the  
Assistant Commissioner for Patents, Washington, D.C.  
20231.

  
Signature of Person Mailing Correspondence

Kay Clavenna

Typed or Printed Name of Person Mailing Correspondence

CC:



## UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
WASHINGTON, D.C. 20231  
www.uspto.gov

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
10/062,853	01/31/2002	James Kleinsteinber	112-0019US

CONFIRMATION NO. 1224

29855  
WONG, CABELLO, LUTSCH, RUTHERFORD & BRUCCULERI,  
P.C.  
20333 SH 249  
SUITE 600  
HOUSTON, TX 77070

## FORMALITIES LETTER



"0C000000007549775"

Date Mailed: 02/28/2002



## NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

## Filing Date Granted

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing.  
*A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.*
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(l) of \$130 for a non-small entity, must be submitted with the missing items identified in this letter.
- The balance due by applicant is \$ 130.

---

*A copy of this notice MUST be returned with the reply.*

Haimant Teghian  
Customer Service Center

Initial Patent Examination Division (703) 308-1202

PART 2 - COPY TO BE RETURNED WITH RESPONSE

<b>DECLARATION FOR UTILITY OR DESIGN</b> <b>PATENT APPLICATION</b> <b>(37 CFR 1.63)</b>	<b>Attorney Docket Number</b> 112-0019US	
	<b>First Named Inventor</b> James Kleinsteinber	
	<b>COMPLETE IF KNOWN</b>	
	<b>Application Number</b>	10 / 062,853
	<b>Filing Date</b>	1/31/2002
<b>Group Art Unit</b>		
<b>Examiner Name</b>		

☐ Declaration Submitted with Initial Filing
 OR
 ☒ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16(e)) required)



As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

NODE AND PORT AUTHENTICATION IN A FIBRE CHANNEL NETWORK

the specification of which (Title of the Invention)

☐ is attached hereto

OR

☒ was filed on (MM/DD/YYYY) 1/31/2002 as United States Application Number or PCT International

Application Number 10/062,853 and was amended on (MM/DD/YYYY) (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or any PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
			<input type="checkbox"/>	YES	NO
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)	
60/334,417	11/30/2001	<input type="checkbox"/> Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 1 of 2]

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

# DECLARATION — Utility or Design Patent Application

Direct all correspondence to:

☒ Customer Number  
or Bar Code Label

29855

OR ☐ Correspondence address below

Name

Address

Address

City

State

ZIP

Country

Telephone

Fax

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR :

☐ A petition has been filed for this unsigned inventor

Given Name

(first and middle (if any)) James

Family Name  
or Surname

Kleinstelber

Inventor's  
Signature

*James Kleinstelber*

Date 5/16/2002

Residence: City San Jose

State CA

Country USA

Citizenship US

Mailing Address 1694 Andalusia Way

Mailing Address

City San Jose

State CA

ZIP 95125

Country USA

NAME OF SECOND INVENTOR:

☐ A petition has been filed for this unsigned inventor

Given Name

(first and middle (if any)) Richard L.

Family Name  
or Surname

Hannons

Inventor's  
Signature

*Richard L. Hannons*

Date 5/16/02

Residence: City Hollister

State CA

Country USA

Citizenship US

Mailing Address 115 Jeanette Court

Mailing Address

City Hollister

State CA


ZIP 95023

Country USA

☐ Additional inventors are being named on the \_\_\_\_\_ supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

**DECLARATION****ADDITIONAL INVENTOR(S)**  
**Supplemental Sheet**  
Page 3 of 3

<b>Name of Additional Joint Inventor, if any:</b>				<input type="checkbox"/> A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any))			Family Name or Surname		
Dilip			Gunawardena		
Inventor's Signature				Date	
Residence: City	Redwood Shores	State	CA	Country	USA
Mailing Address		827 Newport Circle			
Mailing Address					
City	Redwood Shores	State	CA	ZIP	94065
		Country	USA		
<b>Name of Additional Joint Inventor, if any:</b>				<input type="checkbox"/> A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any))			Family Name or Surname		
Shankar			Balasubramanian		
Inventor's Signature				Date 05/16/2002	
Residence: City	Sunnyvale	State	CA	Country	USA
Mailing Address		718 Hebrides Way			
Mailing Address					
City	Sunnyvale	State	CA	ZIP	94087
		Country	USA		
<b>Name of Additional Joint Inventor, if any:</b>				<input type="checkbox"/> A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any))			Family Name or Surname		
Inventor's Signature				Date	
Residence: City		State		Country	
Mailing Address					
Mailing Address					
City		State		ZIP	
		Country			

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box ☐

PTO/SB/81 (02-91)

Approved for use through 10/31/2002 OMB 0651-0035

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

## POWER OF ATTORNEY OR AUTHORIZATION OF AGENT

Application Number	10/062,853
Filing Date	1/31/2002
First Named Inventor	James Kleinsteinber
Group Art Unit	
Examiner Name	
Attorney Docket Number	1120-0019US

I hereby appoint:

☒ Practitioners at Customer Number

29855

Place Customer  
Number Bar Code  
Label here

OR

☐ Practitioner(s) named below:

Name	Registration Number

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR

☐ Practitioner(s) at Customer Number.

Place Customer  
Number Bar Code  
Label here

OR

☐ Firm or  
Individual Name

Address

Address

City

State

Zip

Country

Telephone

Fax

I am the:

☐ Applicant/Inventor.

☒ Assignee of record of the entire interest. See 37 CFR 3.71.  
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

### SIGNATURE of Applicant or Assignee of Record

Name

Ronald Epstein

Signature

Date

3/19/02

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple

☐ Total of \_\_\_\_\_ forms are submitted.

Burden Hour Statement: This form is estimated to take 3 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

**STATEMENT UNDER 37 CFR 3.73(b)**



Applicant: James Kleinstein

Application No.: 10/062,853 Filed: 1/31/2002

Entitled: Node and Port Authentication in a Fibre Channel Network

Brocade Communications Systems, Inc., a Delaware corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest; or

2. ☐ an assignee of an undivided part interest

in the patent application identified above by virtue of either:

A. ☒ An assignment from the inventor(s) of the patent application identified above. The assignment was recorded in the Patent and Trademark Office at Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

OR

B. ☐ A chain of title from the inventor(s), of the patent application identified above, to the current assignee as shown below:

1. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

2. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

3. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet.

☐ Copies of assignments or other documents in the chain of title are attached.

The undersigned (whose title is supplied below) is empowered to sign this statement on behalf of the assignee.

3/19/02  
Date

Signature

Ronald Epstein

Typed or printed name

Vice President and General Counsel

Title

000918

Amt

Inv# Amt

Inv#

40.00

Inv# 05282002F

DATE : May 28, 2002

CHE # : 918

AMOUNT : \$40.00

ACCOUNT : 1

PAID TO : Commissioner of Patents  
Washington, DC 20231

EXPLANATION : Assignment

Wong, Cabello, Lutsch, Rutherford

20333 SH 249, Ste. 600  
Houston, TX 77070

PAY TO THE ORDER OF

Commissioner of Patents  
Washington, DC 20231

COMPASS BANK

Houston, Texas

35-1054/130

876

CHECK NO.

000918

\*\*\* Forty \*\*\*

00/100

May 28, 2002

DATE

AMOUNT \$40.00

⑈000918⑈ ⑆13010547⑆ 84013595⑈



Form PTO-1595

(Rev. 03/01)

OMB No. 0651-0027 (exp. 5/31/2002)

## RECORDATION FORM COVER SHEET

U.S. DEPARTMENT OF COMMERCE

U.S. Patent and Trademark Office

## PATENTS ONLY

Tab settings

To the Honorable Commissioner of Patents and Trademarks: Please record the attached original documents or copy thereof.

## 1. Name of conveying party(ies):

James Kleinstein;  
Richard L. Hammon;  
Dilip Gunawardena;  
Shankar Balasubramanian

Additional name(s) of conveying party(ies) attached? ☐ Yes ☒ No

## 3. Nature of conveyance:

- ☒ Assignment ☐ Merger  
☐ Security Agreement ☐ Change of Name  
☐ Other

Execution Date: 5/16/2002

## 2. Name and address of receiving party(ies)

Name: Brocade Communications Systems, Inc.

Internal Address:

Street Address: 1745 Technology Drive

City: San Jose State: CA Zip: 95110

Additional name(s) & address(es) attached? ☐ Yes ☒ No

## 4. Application number(s) or patent number(s):

If this document is being filed together with a new application, the execution date of the application is:

A. Patent Application No.(s)  
10/062,853

B. Patent No.(s)

Additional numbers attached? ☐ Yes ☒ No

## 5. Name and address of party to whom correspondence concerning document should be mailed:

Name: Keith Lutsch

Internal Address: Wong Cabello Lutsch

Rutherford &amp; Bruculeri PC

Street Address: 20333 SH 249, Suite 600

City: Houston State: TX Zip: 77070

## 6. Total number of applications and patents involved: 1

7. Total fee (37 CFR 3.41).....\$40.00

☒ Enclosed☐ Authorized to be charged to deposit account

## 8. Deposit account number:

501922

(Attach duplicate copy of this page if paying by deposit account)

## DO NOT USE THIS SPACE

## 9. Statement and signature.

To the best of my knowledge and belief, the foregoing information is true and correct and any attached copy is a true copy of the original document.

Louis Bruculeri

Name of Person Signing

Signature

5/16/2002

Date

Total number of pages including cover sheet, attachments, and documents: 5

## ASSIGNMENT

For good and valuable consideration, the receipt of which is hereby acknowledged, the person(s) named below (referred to as "INVENTOR" whether singular or plural) has sold, assigned, and transferred and does hereby sell, assign, and transfer to Brocade Communications Systems, Inc., a Delaware corporation, having a place of business at 1745 Technology Drive, San Jose, California 95110 ("ASSIGNEE"), for itself and its successors, transferees, and assignees, the following:

The entire worldwide right, title, and interest in all inventions and improvements ("SUBJECT MATTER") that are disclosed in the application for United States Letters Patent entitled: NODE AND PORT AUTHENTICATION IN A FIBRE CHANNEL NETWORK ("APPLICATION"), which:

- ☐ is to be filed herewith
- ☒ was filed on January 31, 2002, now bearing U.S. Serial Number 10/062,853 and for which a Declaration was executed by INVENTOR on the date(s) below; and

The entire worldwide right, title, and interest in and to (a) the APPLICATION, including any right of priority; (b) any divisional, continuation, substitute, renewal, reissue, and other related applications thereto which have been or may be filed in the United States or elsewhere in the world; and (c) patents which may be granted on the applications set forth in (a) and (b) above.

INVENTOR agrees that ASSIGNEE may apply for and receive patents for SUBJECT MATTER in ASSIGNEE's own name.

INVENTOR agrees to do the following, when requested, and without further consideration, in order to carry out the intent of this Assignment: (1) execute all oaths, assignments, powers of attorney, applications, and other papers necessary or desirable to fully secure to ASSIGNEE the rights, titles, and interests herein conveyed; (2) communicate to ASSIGNEE all known facts relating to the SUBJECT MATTER; and (3) generally do all lawful acts that ASSIGNEE shall consider desirable for securing, maintaining, and enforcing worldwide patent protection relating to the SUBJECT MATTER and for vesting in ASSIGNEE the rights, titles, and interests herein conveyed. INVENTOR further agrees to provide any successor, assign, or legal representative of ASSIGNEE with the benefits and assistance provided to ASSIGNEE hereunder.

INVENTOR represents that INVENTOR has the rights, titles, and interests to convey as set forth herein, and covenants with ASSIGNEE that the INVENTOR has made or will make hereafter no assignment, grant, mortgage, license, or other agreement affecting the rights, titles, and interests herein conveyed.

This Assignment may be executed in one or more counterparts, each of which shall be deemed an original and all of which may be taken together as one and the same Assignment.

Executed this 16<sup>th</sup> day of May, 2002.

James K Kleinsteinber  
James Kleinsteinber

STATE OF CALIFORNIA

COUNTY OF Santa Clara

BEFORE ME, the undersigned authority, on this day personally appeared James Kleinsteinber, known to me to be the person whose name is subscribed to the foregoing instrument, and acknowledged to me that he/she executed the same for the purposes and consideration herein expressed.

GIVEN UNDER MY HAND and seal of office this 16<sup>th</sup> day of May, 2002.



Elizabeth Moore  
Notary Public in and for the  
State of California

\*\*\*\*\*

Executed this 16<sup>th</sup> day of May, 2002.

Richard L. Hammons  
Richard L. Hammons

STATE OF CALIFORNIA

COUNTY OF Santa Clara

BEFORE ME, the undersigned authority, on this day personally appeared Richard L. Hammons, known to me to be the person whose name is subscribed to the foregoing instrument, and acknowledged to me that he/she executed the same for the purposes and consideration herein expressed.

GIVEN UNDER MY HAND and seal of office this 16<sup>th</sup> day of May, 2002.



Elizabeth Moore  
Notary Public in and for the  
State of California

\*\*\*\*\*

Executed this 10<sup>th</sup> day of May, 2002.

\_\_\_\_\_  
Dilip Gunawardena

STATE OF CALIFORNIA

COUNTY OF \_\_\_\_\_

BEFORE ME, the undersigned authority, on this day personally appeared Dilip Gunawardena, known to me to be the person whose name is subscribed to the foregoing instrument, and acknowledged to me that he/she executed the same for the purposes and consideration herein expressed.

GIVEN UNDER MY HAND and seal of office this \_\_\_\_ day of \_\_\_\_\_, 2002.

\_\_\_\_\_  
Notary Public in and for the  
State of California

\*\*\*\*\*

Executed this 11<sup>th</sup> day of May, 2002.

Shankar Balasubramanian

STATE OF CALIFORNIA

COUNTY OF Santa Clara

BEFORE ME, the undersigned authority, on this day personally appeared Shankar Balasubramanian, known to me to be the person whose name is subscribed to the foregoing instrument, and acknowledged to me that he/she executed the same for the purposes and consideration herein expressed.

GIVEN UNDER MY HAND and seal of office this 16th day of May, 2002.



Elizabeth Moore  
Notary Public in and for the  
State of California

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Applicant:

James Kleinstein  
Richard L. Hammons  
Dilip Gunawardena  
Shankar Balasubramanian

Serial No. 10/062,853

Filed: January 31, 2002

For: NODE AND PORT  
AUTHENTICATION IN A  
FIBRE CHANNEL NETWORK



Docket No. 112-0019US

Art Unit

Examiner:

Declaration of Louis Brucculeri in Support of Petition under § 1.47

1. My name is Louis Brucculeri. I am an attorney at the law firm of Wong, Cabello, Lutsch, Rutherford & Brucculeri, P.C., 20333 SH 249, Suite 600, Houston, Texas 77070. I am a member of the State Bar of Texas having bar number 00783737. I am a registered patent attorney, registration number 38,834.
2. I represent Brocade Communications Systems Incorporated in the prosecution of the subject patent application.
3. I have investigated at Applicant's business and determined that Dilip Gunawardena is Applicant's ex-employee and a person that Applicant believes is an inventor of the subject application.
4. Over a five-week period, I have attempted to solicit cooperation from Mr. Gunawardena regarding the subject application. During this period, I have spoken by phone with Mr. Gunawardena several times, written three letters to Mr. Gunawardena and sent several emails.
5. Other than during phone conversations, Mr. Gunawardena has refused to respond substantively. For example, all the emails sent to me by Mr. Gunawardena are limited to requests for phone calls and associated phone call scheduling

6. I spoke to Mr. Gunawardena regarding the subject application on April 5, 2002.

A. I explained that Brocade had filed the subject patent application and that we believed he was an inventor.

B. He agreed that he was a past contractor and past employee of Brocade.

C. He suggested that he would desire an upfront payment and a royalty in order to be cooperative regarding subject application.

D. I explained that his employment agreement would have given his commitment to cooperate.

E. We agreed that he would need or want to understand his employment agreement in order to determine what to do.

7. On Monday, April 8, I sent Mr. Gunawardena a copy of his employment agreement. The Employment Agreement is attached to this declaration as Exhibit I and contains, a §3 "Inventions." In §3, Mr. Gunawardena assigns all inventions to Applicant without royalties and agrees to cooperate with prosecution after termination of employment.

8. On Tuesday, April 16, 2002, I spoke again by phone with Mr. Gunawardena.

A. Mr. Gunawardena conceded that Brocade was the first to ever use port authentication of any kind in a fabric environment.

B. Mr. Gunawardena further conceded that Brocade was the first to use port authentication of any kind in a Fibre Channel environment.

C. While Mr. Gunawardena had not yet seen the patent application, he generally conveyed that the application would be invalid without his cooperation.

D. Mr. Gunawardena offered his assistance with the applications for \$250,000.000 paid over two years. The specifics of Mr. Gunawardena's offer are in My April 17 letters, attached along with Federal Express documents as Exhibit 2.

E. After drafting the April 17 letters, I again spoke to Mr. Gunawardena to reach agreement on the wording of his \$250,000 offer.

F. While on the phone, I read to him my draft and he made several edits (all of which are incorporated in Exhibit 2).

G. Mr. Gunawardena stated that he would take legal action if Brocade attempted to go forward without meeting the terms of his \$250,000 offer.

9. On Monday April 22 I spoke again to Mr. Gunawardena.

A. He confirmed that my letter of April 17 (Exhibit 2) was an accurate description of his proposal

B. He conveyed that, if Brocade did not accept his offer, he would spend "millions" of his own money to make sure that a valid patent does not issue.

10. On Friday, May 10, I spoke again to Mr. Gunawardena.

A. He wanted to remind me that his offer was non-negotiable and that after May 31, there would be no further opportunity for discussion.

B. I told him that I sent a package on that day containing Brocade's proposal and a copy of the application and associated papers.

11. On Friday, May 10, I sent a copy of the application, declaration papers and assignment papers to Mr. Gunawardena. The copy of my letter is enclosed as Exhibit 3. Generally, the letter requests Mr. Gunawardena's cooperation and offers him up to \$200 per hour (to a maximum of \$2000) to read the application and sign the papers if appropriate. The package sent included return Federal Express materials and a form for Mr. Gunawardena to expressly accept or reject Brocade's offer. Receipt of the material by Mr. Gunawardena on May 13, 2002 at 11:03 a.m. was verified by checking with Federal Express.

12. On Tuesday, May 13, I spoke to Mr. Gunawardena again.

A. He confirmed receipt of the package I sent on May 10.

B. He declined Brocade's offer and reiterated his refusal to cooperate unless Brocade met the precise terms of his \$250,000.00 offer.

13. Mr. Gunawardena has not returned any material as of the date of this declaration.

14. During my various conversations with Mr. Gunawardena, he made numerous remarks concerning the potential validity or scope of a patent drawn in this

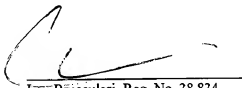


area of technology. I have not recounted those comments because they are not relevant to Mr. Gunawardena's refusal to cooperate in prosecution.

15. In summary, on several occasions and over several conversations, Mr. Gunawardena declined to cooperate with the prosecution of the subject application in any respect (even to send a letter back to me), unless Brocade agreed to the terms of his \$250,000 offer.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

May 18, 2002

  
\_\_\_\_\_  
Lou Bruculeri, Reg. No. 38,834

Wong, Cabello, Lutsch,  
Rutherford & Bruculeri, P.C.  
20333 SH 249, Suite 600  
Houston, TX 77070  
832/446-2415  
Fax 832/446-2424



## UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents  
United States Patent and Trademark Office  
Washington, D.C. 20231  
www.uspto.gov

Paper No. 5

WONG, CABELLO, LUTSCH,  
RUTHERFORD & BRUCCULERI, P.C.  
20333 SH 249  
SUITE 600  
HOUSTON, TX 77070

RECEIVED  
WONG CABELLO

AUG 27 2002

COPY MAILED

AUG 23 2002

OFFICE OF PETITIONS

DOCKETED BY  
ACTION  
CLUE DATE

In re Application of  
James Kleinsteinber,  
Richard L. Hammons,  
Dilip Gunawardena, and  
Shankar Balasubramanian  
Application No. 10/062,853  
Filed: January 31, 2002  
Attorney Docket No. 112-0019US  
Title: Node and Port Authentication:  
in a Fibre Channel Network

DECISION ACCORDING STATUS  
UNDER 37 C.F.R. §1.47(a)

This is in response to the petition, filed June 6, 2002  
(certificate of mailing May 28, 2002), under 37 CFR 1.47(a).

The petition is **GRANTED**.

The above-identified application was filed on January 31, 2002, without an executed oath or declaration. James Kleinsteinber, Richard L. Hammons, Dilip Gunawardena, and Shankar Balasubramanian were named as joint inventors. Accordingly, on February 28, 2002, applicants were mailed a "Notice to File Missing Parts of Nonprovisional Application - Filing Date Granted," requiring an executed oath or declaration, and the surcharge under §1.16(e) for late filing. This Notice set a two-month period for reply with extensions of time obtainable under §1.136(a).

In reply, rule 47 applicants filed the instant petition, paid both the petition fee (§130) and the surcharge under §1.16(e) (§130), and submitted a petition for a one-month extension of time to make the reply timely. Applicants assert that status under §1.47 is proper because inventor Gunawardena refuses to join in the application. In support thereof, applicants submitted *inter alia* a declaration of patent attorney Louis Brucculeri with documentary evidence of the presentation of the application papers for signature to inventor Gunawardena.

A grantable petition under 37 CFR 1.47(a) requires: (1) proof that the non-signing inventor cannot be reached or refuses to sign the oath or declaration after having been presented with the application papers (specification, claims and drawings); (2) an acceptable oath or declaration in compliance with 35 U.S.C. §§115 and 116; (3) the petition fee; and (4) a statement of the last known address of the non-signing inventor(s).

By declaration of Louis Brucculeri and supporting documentary evidence, applicants have shown that a bona fide attempt was made to present a copy of the application papers (specification, including claims, drawings, and oath or declaration) to the non-signing inventor, and that inventor Gunawardena has refused to join in the application. Accompanying the petition is a declaration executed by joint inventors Kleinsteinber, Hammons, and Balasubramanian on behalf of themselves and on behalf of non-signing inventor Gunawardena. Moreover, the petition submitted included the petition fee and a statement of the last known address of inventor Gunawardena.

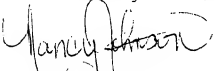
This declaration filed June 6, 2002 has been reviewed and found in compliance with \$1.63. The petition likewise is in compliance with \$1.47.

In view thereof, this application is hereby accorded Rule 1.47(a) status.

As provided in new Rule 1.47(c), this Office will forward notice of this application's filing to the non-signing inventor at the address given in the petition. Notice of the filing of this application will also be published in the Official Gazette.

The application file is being forwarded to Technology Center 2131 for examination.

Telephone inquiries regarding this decision should be directed to the undersigned at (703) 305-0309.

  
Nancy Johnson  
Petitions Attorney  
Office of Petitions  
Office of the Deputy Commissioner  
for Patent Examination Policy